智能审计技术在财务舞弊识别中的应用

王金红，杨焕云

（聊城大学商学院，聊城 252000）

摘要：财务舞弊手段的隐蔽化、复杂化发展，对传统审计的识别能力与效率提出严峻挑战。智能审计技术凭借数据处理与分析优势，为破解财务舞弊识别难题提供了新路径。以财务舞弊识别为特定场景，以舞弊 GONE(贪婪、机会、需要和暴露)理论为基础，构建“事前预防-事中监控-事后核查”的全流程智能审计应用框架，系统整合机器人流程自动化(RPA)、自然语言处理(NLP)、北斗定位、知识图谱与机器学习等技术，针对虚增收入、存货造假、资金体外循环等典型舞弊场景，展开场景化分析。研究表明，智能审计可实现从“抽样审计”到“全量审计”、从“经验判断”到“数据驱动”、从“事后追溯”向“事前预防＋事中监控”的模式升级。同时，进一步揭示了智能审计在舞弊识别落地中的现实困境。研究成果为智能审计在财务舞弊识别中的合规化、规模化应用提供了理论支撑与实践参考，助力提升资本市场审计监督效能。

关键词：智能审计；财务舞弊识别；风险防控；舞弊 GONE(贪婪、机会、需要和暴露)理论

中图分类号：F239.1；F239.4 **文献标志码：**A **文章编号：**1671－1807(2026)15－0026－06

财务舞弊是资本市场的“毒瘤”，不仅严重侵蚀投资者合法权益、破坏市场公平交易秩序，更会扭曲资源配置效率、动摇资本市场信用根基。近年来，上市公司财务舞弊案件频发，据中国证监会行政处罚数据统计，2023—2025 年累计披露上市公司财务舞弊相关行政处罚决定书超 200 份。与此同时，传统财务舞弊识别方式存在明显短板：①人工审计效率低下，面对海量财务数据与复杂业务链条，难以实现全量覆盖，易出现遗漏性风险；②识别手段滞后，多依赖事后抽样检查、人工经验判断，对舞弊的事前预警与事中监控能力不足[1]；③应对新型舞弊乏力，面对数字化背景下的财务数据篡改、系统漏洞利用等新型舞弊手段，传统方法缺乏针对性与有效性。

在此背景下，智能审计技术凭借大数据、人工智能、区块链等核心技术优势，为破解财务舞弊识别难题提供了全新路径。智能审计技术包括机器学习、自然语言处理(natural language processing，NLP)、异常检测算法、知识图谱、机器人流程自动化(robotic process automation，RPA)等，能够对企业的财务数据、资金流水、业务单据、合同文本、公告信息等进行全量采集、多维度交叉验证和实时风险预警。与传统方式相比，智能审计实现了 3 个转变：从“抽样”到“全量”，从“事后”到“实时”，从“经验判断”到“数据驱动”，展示了人工智能在创造力和复杂任务处理中的巨大潜力[2]。然而，智能审计并非万能，其有效性高度依赖数据质量、算法适配性与人机协同机制。因此，深入研究智能审计在财务舞弊识别中的具体应用逻辑与现实困境具有重要的理论价值与实践意义。

1 文献综述

随着大数据、人工智能技术的快速迭代，审计行业迎来数字化转型的关键机遇，人工智能与审计领域的融合应用成为国内外学者的研究热点。现有研究围绕人工智能技术在审计中的应用价值、实践路径、现存问题及优化策略展开了多维度探讨，为智能审计技术在财务舞弊识别中的专项应用奠定了坚实的理论与实践基础，同时也暴露了研究局限，为研究提供了理论参考与改进方向。

1.1 国外文献综述

现有研究虽广泛探讨了人工智能在审计中的应用，但直接聚焦于财务舞弊识别场景的成果相对有限，且多集中于技术可行性的宏观层面。Greenman 等[3]从行业变革视角指出，人工智能技术正在自动化常规任务、增强自动分析能力，人工智能的采用正在重塑会计人员和审计人员的角色，推动其从重复性的基础工作中解放出来，更多聚焦风险管理、战略制定等高阶工作，为理解技术驱动下的行业转型提供了宏观框架。

收稿日期：2026-04-16

作者简介：王金红(2002—)，女，山东滨州人，硕士研究生，研究方向为财务会计；通信作者杨焕云(1976—)，女，山东阳谷人，硕士，副教授，研究方向为财务会计理论与实务。

在更为聚焦的研究中,部分学者开始探索技术在具体审计环节的应用,但其针对性仍显不足。Pan[4]以审计计划阶段的核心环节——审计风险识别为切入点,提出依托大型语言模型(large language models,LLMs)的自然语言处理能力,结合智能代理(Agents)的自动化执行特性构建协同工作机制,以处理多源数据、定位关键审计风险。该方法为 Greenman 等[3]预判的审计师角色转型提供了具体场景支撑。然而,该研究并未进一步深入到"如何利用这些技术识别特定财务舞弊手法"的层面。Lin[5]则从宏观层面系统研判了人工智能审计的发展态势,总结了其在提升审计效率、质量与推动审计模式创新方面的机遇,剖析应用挑战并提出应对策略,完善了人工智能审计研究的整体体系,但同样未对财务舞弊识别这一特定场景进行深入剖析。

综上,国外研究虽验证了人工智能在审计领域的应用价值,构建了从技术潜力到行业影响的研究体系,但仍存在明显不足:①研究视角偏泛化,对财务舞弊识别这一细分场景的针对性研究较少;②尚未形成智能审计技术与财务舞弊典型手段的对应适配研究,技术应用的场景化落地仍存在空白,这也为本文的研究提供了切入点。

1.2 国内文献综述

国内学者紧跟国际前沿,结合人工智能在审计实践中的应用,形成了"技术应用-问题剖析-对策优化"的研究框架,但同样存在对财务舞弊识别场景聚焦不足的问题。

在人工智能对审计行业的变革层面,研究从技术引入逐步走向决策重构。秦荣生[6]指出,大数据、云计算作为人工智能的核心支撑技术,为现代审计提供了全新思路。在此基础上,龙志能等[7]遵循审计业务逻辑,系统剖析了人工智能的作用机制,构建了人工智能驱动的审计决策分析框架。这一脉络体现了从"技术赋能"到"决策重构"的深化。

在具体应用层面,研究从技术验证转向实务落地。戚啸艳等[8]梳理了国际"四大"会计师事务所的探索实践,发现机器学习、NLP、RPA 等技术已被广泛嵌入审计流程。邓亦玮等[9]进一步提出,人工智能可通过自动化处理海量数据、深度学习算法识别异常、NLP 优化报告生成等路径,推动审计智能化。这些研究共同勾勒出技术赋能审计的具体路径。

然而,当研究视角转向财务舞弊识别这一具体任务时,现有文献的局限性便凸显出来。多数研究停留在"人工智能可识别异常交易"或"人工智能能提升审计效率"的宽泛结论上,缺乏对"虚增收入""存货造假""资金体外循环"等典型舞弊手法与机器学习、NLP 等特定技术之间精准映射关系的系统性构建。例如,杨寅[10]总结了人工智能审计的核心优势,包括提升审计效率、降低审计成本、增强风险识别客观性与准确性等。同时,吴勇等[11]系统辨识了智能审计面临的复杂挑战,并提出综合性对策,但均未深入探讨智能审计技术如何应用于财务舞弊识别这一细分场景。

1.3 文献述评

国内外研究已从技术可行性、行业变革等维度验证了人工智能在审计中的价值,形成了从宏观到微观、从技术到制度的研究链条。然而,现有研究仍存在两方面的明显不足:①研究视角泛化,多数成果讨论"人工智能+审计"的整体效能,对财务舞弊识别这一高频刚需场景的针对性研究不足;②技术应用与舞弊手段之间缺乏精准映射,尚未建立虚增收入、资金体外循环、存货造假等典型舞弊行为与机器学习、图神经网络、NLP 等特定技术的对应关系,导致技术选型缺乏理论依据。基于上述空白,现聚焦财务舞弊识别场景,构建"舞弊手段-智能技术-审计阶段"的三维分析框架,并结合案例揭示各技术的具体识别逻辑,旨在填补从"技术能做什么"到"技术具体怎么做"的研究空白。

2 理论基础与分析框架

2.1 财务舞弊 GONE 理论

GONE(greed, opportunity, need, and exposure,贪婪、机会、需要和暴露)理论指出,当管理层存在逐利动机与业绩压力,同时内部控制存在漏洞、舞弊暴露概率较低时,财务造假极易发生[12]。智能审计对财务舞弊的 4 个因子分别实施干预:针对贪婪,通过关联方交易图谱挖掘隐性利益输送;针对机会,利用 RPA 对审批流程进行全量自动化测试,标记"无审批付款"等控制缺失;针对需要,结合 NLP 语调分析与行业对比,识别"逆行业增长"等异常动机;针对暴露,通过全量数据存证与异常行为追溯,大幅提高舞弊被发现的风险。由此,智能审计从源头上压缩舞弊空间。

2.2 技术:舞弊手段映射

在财务舞弊识别中,智能审计技术并非笼统地"识别异常",而是针对不同舞弊手段采用差异化的技术路径。表 1 概括了核心技术及其对应的舞弊识别逻辑。

表 1　核心技术及其对应的舞弊识别逻辑

技术	核心功能	识别的舞弊手段	识别逻辑示例
监督学习[随机森林、XGBoost（极限梯度提升）]	基于历史标签数据训练分类模型	虚增收入、隐瞒费用、资产造假	输入企业历年财务比率（收入增速、毛利率、应收周转率等），模型输出舞弊概率，并利用 SHAP（沙普利加性解释）值解释哪些指标驱动了高风险判断
无监督学习（孤立森林、*K*-means 聚类）	无需标签，发现数据中的异常簇	异常交易、非常规资金流动	对全量订单按金额、时间、渠道聚类，自动将“凌晨高频整数倍订单”归为异常簇，提示虚构交易
自然语言处理（NLP）	文本语义分析、情感识别、矛盾检测	信息披露隐瞒、前后表述不一致	计算历年公告的向量相似度，发现“冷水团致绝收”与“水温适宜生长”等语义矛盾；识别管理层语调异常乐观但财务数据恶化
图神经网络/知识图谱	挖掘多实体间的关联关系	关联方非公允交易、资金体外循环	构建“企业-股东-供应商-银行账户”图谱，遍历资金链路，发现 A→B→C→A 的闭环路径且无真实货物交付
机器人流程自动化（RPA）	模拟人工操作，全量自动比对	伪造原始凭证、篡改银行流水	自动登录财务系统下载全部凭证，与税务系统发票数据逐行比对，标记金额、对方账户、日期不一致的记录
图像识别[RFID（射频识别）、卫星遥感]	资产物理位置追踪、实物盘点	虚增存货（如生物资产）、虚构工程量	利用卫星遥感或无人机影像比对工程进度与账面；通过 RFID 或北斗定位追踪生物资产（如扇贝）采捕轨迹，验证存货真实性

3　智能审计技术在财务舞弊识别中的应用场景

3.1　事前预防：基于多维指标的异常风险预测

事前预防的核心是利用历史数据训练预测模型，在企业年度报告发布前或审计计划制订阶段，借助监督学习模型对历史数据进行训练，输出各企业的舞弊风险评分，从而将审计资源优先配置到高风险区域。在具体实践中通常采用随机森林或逻辑回归等监督学习算法构建评估体系，在输入企业多维风险特征数据时，重点围绕收入、存货和应收账款 3 个高风险领域构建专属指标体系，以此提升风险识别的针对性与精准度。

在收入方面，系统采集“营业收入增长率、毛利率波动幅度、经营活动现金流与收入比值”等指标。若某消费类企业营业收入连续两年增速超过 30%（显著高于行业平均增速的阈值），但同期经营现金流增速不足 5%，且毛利率在行业整体下滑时仍保持稳定，模型将其判定为高风险。

针对存货，模型关注“存货周转天数、存货跌价准备计提比例、仓库盘点差异率”等指标。若某商贸企业存货周转天数由 45 d 延长至 90 d，同时盘点差异率达 6.5%，模型判定其为高风险。

对于应收账款，模型分析“应收账款周转天数、长账龄占比（3 年以上）、坏账准备计提比例”等指标。例如，某软件企业应收账款周转天数从 60 d 增至 120 d，且 3 年以上账龄应收账款占比超过 35%，模型将其列为重点审计对象。

据文献研究，会计师事务所借助 AI 技术可在 24 h 内完成范围界定，高风险领域命中率从约 55% 提升至 95%，人工投入从 9 人/d 降至 0.5 人/d，大幅减少盲目审计带来的无效工作量[13]。

3.2　事中监控：交易与资金流向的实时分析

事中监控依托实时交易数据开展动态监测，在舞弊行为发生过程中及时捕捉异常特征并发出预警。人工智能技术通过搭建资金流向监测平台，可自动采集并整合银行流水、第三方支付记录、ERP（企业资源计划）业务订单等多源数据，运用 *K*-means聚类、孤立森林等无监督学习方法对全量交易数据开展离群点检测，精准识别金额异常、时间分布异常、交易对手异常等典型问题。同时借助图神经网络构建交易关联网络，对资金流转路径进行全面追溯，有效识别 A→B→C→A 这类闭环式虚假交易模式。

在实时风险判断环节，智能审计能够结合舞弊 GONE 理论捕捉多维风险信号，实现风险的实时预警。在关联交易管理中，自然语言处理技术可对合同条款进行深度解析，识别“定价依据模糊”“交易对手为空壳公司”等反映机会因子的信号，异常检测模型也会对关联方资金拆借不计息等反映需要因子的异常情况进行持续监测，同时重点关注管理层异常贪婪动机与舞弊暴露概率较低的隐蔽环节。在存货管理方面，智能审计系统对接企业仓储管理系统，提取并分析出入库操作日志、盘点记录等全流程业务数据，及时发现“夜间无审批擅自入库”“同一批次存货短时间内重复盘点”等内控漏洞。系统还会对比存货周转天数与营业收入增速的匹配性，当企业出现存货周转天数明显延长而营业收入逆势高速增长的矛盾状态时，将自动触发虚增存货相关预警。在应收账款管理领域，系统整合销售合同与回款流水信息，重点筛查缺乏真实交易背景

以及回款资金异常转入关联方账户的违规情形。借助人工智能技术的全面赋能,审计风险预警实现了从“事后救火”向“事中实时监测”的重要转变。

在控制测试环节,无监督学习算法能够对全部审批单据开展合规性与异常性分类。例如,在部分企业的关联交易审批流程中,系统可自动识别仅经单人审批的异常记录并进行重点标注。RPA 技术也可模拟人工操作,对关联交易多级审批、存货双人交叉盘点、应收账款定期对账等标准化流程开展自动化校验。经过智能化审计优化,控制测试覆盖率可由传统审计模式下的 30%～50%提升至 100%,测试耗时缩短 50%[14]。

在实质性程序中,智能审计依托图神经网络搭建专项证据图谱:在关联交易场景构建“关联方-交易合同-资金流-物流单”关联图谱,还原虚增收入的完整交易闭环;在存货管理场景搭建“采购订单-入库单-出库单-物流信息-盘点记录”全流程图谱,精准识别存货空转等舞弊行为;在应收账款场景构建“销售订单-应收账款-回款记录-资金流向”关系图谱,有效发现虚假回款问题。

3.3 事后核查:全量证据挖掘

在财务舞弊已发生、进入年度审计或监管调查阶段,事后核查的核心价值在于依托自动化工具、文本语义分析及空间可视化技术,对全部凭证、公告文本、物理轨迹开展多维全面审查,精准捕捉人工抽样审计难以察觉的细节证据,最终形成可追溯、可交互的完整证据链,为舞弊认定与问题整改提供坚实支撑。这一环节解决了传统审计“取证难、验证慢、覆盖不全”的痛点,综合运用 RPA、NLP、北斗卫星定位、知识图谱及数据可视化等多项智能技术,构建起全流程、多维度的舞弊核查体系,实现审计取证与风险研判的智能化升级。

依托证监会《行政处罚决定书》及权威媒体披露的獐子岛集团股份有限公司(以下简称“獐子岛”)存货虚假记录、减值依据不足等舞弊手法,模拟构建针对性的智能审计事后核查流程。本部分为模拟演示,所涉具体数据为示例,不代表獐子岛的真实审计数据。选择獐子岛作为模拟案例进行分析,主要基于以下考虑:①獐子岛财务舞弊案是利用卫星定位等科技手段进行稽查取证的标志性案例,其存货(扇贝)造假的特殊性对传统审计方法构成了极大挑战,充分体现了在复杂生物资产领域引入智能审计技术的必要性和紧迫性。②该案例涵盖了存货虚增、减值依据不足、信息披露前后矛盾等多种舞弊手法,具有综合性和典型性,能够较为全面地展示事后核查阶段 RPA、NLP、北斗定位等多种智能技术的集成应用逻辑。因此,围绕獐子岛案例构建模拟核查流程,对于验证智能审计框架在复杂场景下的有效性具有较强的示范意义。具体核查工作分为 4 个逻辑层次。

第 1 层:全量凭证与业务记录比对(RPA)。借助 RPA 模拟人工操作,自动登录财务系统逐笔下载会计凭证及附件,与税务电子底账、银行接口数据进行逐行精准比对,快速标记金额、日期、对方账户不一致的异常记录。同时抽取獐子岛 2014—2018 年扇贝底播记录与采捕记录,按海域坐标完成数据关联,如精准识别出 47 个投苗批次、累计6.2 亿元投苗金额在后续 3 年内无任何采捕记录,底播资产凭空“消失”的异常问题,系统自动生成差异清单,提示存货可能被虚增。这一步骤解决了传统审计只能抽查部分记录、无法覆盖全量数据的问题。

第 2 层:公告文本语义分析(NLP)。利用 NLP 技术,对企业公告进行语义分析。通过智能分析模型读取獐子岛 2014—2019 年发布的所有公告,对比不同时期公告的内容相似度。例如 2014 年公告称“北黄海冷水团导致扇贝绝收”,2017 年同一海域公告称“水温适宜、生长良好”,两段文本相似度计算值仅为 0.23(正常同类主题公告相似度均值为 0.65)。模型自动标记为“高风险矛盾”,并在地理关键词“北黄海”“獐子岛海域”上标注正负面描述冲突。同时按照规范要求,核查存货核销公告是否包含第三方检测报告编号、死亡时间、死亡比例、公证记录等关键内容,结果发现 2014 年公告缺少关键编号与公证记录,信息完整度评分仅 41/100(阈值 70),及时提示审计人员追溯原始证据。

第 3 层:北斗定位轨迹核验与知识图谱可视化分析。针对渔业资产的特殊性,仅凭账面和文本分析不足以形成闭环证据。在事后调查阶段,监管机构调取了獐子岛采捕船只的历史北斗卫星定位数据。基于“北斗船位数据提取作业点”技术,系统自动复原每艘船只的真实航行轨迹,并据此推算出实际采捕作业的海域范围与面积。将北斗轨迹数据与公司账面记录的采捕海域进行叠加比对后发现,账面记录的多个高价值采捕区域实际并无船只作业轨迹,而船只频繁作业的部分海域却未在账面上体现。例如,某年度账面记录采捕面积达 12 万亩(1 亩≈667 m^2),但北斗轨迹推算的实际作业面积不足 5 万亩,差异率超过 60%。

与此同时，利用知识图谱技术构建“企业-船只-海域-交易对手-时间”的全景关联图谱，将采捕记录、物流单、资金流等实体与关系可视化。通过图谱分析，发现3艘船只的轨迹在同一时间高度重叠却分别报告采捕不同海域，且对应的采捕记录均无第三方物流单佐证，形成可疑子图。此外，数据可视化技术将数百万条凭证分录，银行流水以散点图、力导向图等形式展示，审计人员可直观发现“同一时段内同一船只出现在多个不相邻海域”等异常模式，极大提升了异常识别效率。

第4层：证据链整合与报告生成。上述3层输出由系统自动汇总，按照“风险等级-舞弊线索-涉及金额-证据来源-整改建议”的结构生成结构化审计底稿。例如，系统输出“高风险-存货虚增：①RPA发现47批次无采捕记录(6.2亿元)；②NLP语义矛盾及信息缺失；③北斗轨迹显示实际采捕面积不足账面的60%；④知识图谱识别出3艘船只作业轨迹冲突。综合证据链完整。建议：调取第三方监测报告，实地核查未作业海域，并追溯相关责任人。整个核查过程从传统人工需要数周压缩至数小时，且覆盖全部数据与物理轨迹。

4 财务舞弊识别中智能审计面临的现实问题

尽管智能审计在技术上展现出显著优势，但在实际落地过程中，仍面临一系列制约因素，且这些问题在财务舞弊识别场景中具有特殊性。

4.1 数据层面的脆弱性

舞弊识别的智能模型需要融合财务、业务、资金、税务、物流等多源数据。然而，舞弊企业本身就有动机篡改数据，这导致训练数据的真实性无法保证。例如，舞弊企业伪造银行回单和存货记录，如果智能审计系统直接使用企业提供的数据库进行训练，就会被“污染”的数据误导，产生“垃圾进、垃圾出”的后果。此外，企业内部系统之间往往存在数据孤岛，ERP系统中的销售订单与财务系统中的收入确认金额不一致，税控系统开票金额与银行收款金额不匹配，这些“正常的不一致”与“舞弊的不一致”难以自动区分，导致大量误报。

4.2 技术层面的深度不足与“黑箱”问题

目前多数会计师事务所和企业的智能审计应用仍停留在“规则引擎＋简单统计”层面，如设置“毛利率波动超过20%触发预警”。这种浅层应用无法应对复杂的、多步骤的舞弊逻辑，如通过多个关联方构建资金循环。而深度神经网络等复杂模型虽然精度高，但其决策过程难以解释。审计工作具有高度合规性要求，审计人员需要向监管机构说明判断依据。如果模型只说“该企业风险评分85分”却无法解释“因为收入与现金流偏离3.2个标准差、关联交易比例超过40%、存货周转天数异常延长”，其结论就难以被采纳。可解释性弱直接制约了智能审计在法定审计程序中的应用。

4.3 人才层面的结构性短缺与人机协同障碍

智能审计需要既懂会计、审计准则、舞弊手法，又懂Python编程、数据库查询、机器学习原理的复合型人才。现实中，传统审计人员大多毕业于会计或财务管理专业，对数理统计和算法逻辑感到陌生；而数据科学人员不了解审计程序、重要性水平、实质性测试等概念，无法设计符合审计准则的分析模型。此外，人机协同模式尚未成熟，部分审计人员对智能工具存在抵触，认为机器会替代其工作；而另一种极端则是过度依赖系统，放弃专业判断。例如，某审计项目组完全接受系统的风险评分，未对“低风险”但存在明显业务逻辑矛盾的企业追加程序，导致漏报。

4.4 制度层面的规范缺失与监管空白

当前中国尚未出台针对智能审计在财务舞弊识别领域的专项技术标准。数据隐私方面，审计过程中需要调取企业银行流水、发票明细等敏感信息，如何在《中华人民共和国个人信息保护法》《中华人民共和国数据安全法》框架下合法使用这些数据，缺乏明确指引。算法责任方面，如果智能审计系统将正常企业误判为舞弊，导致股价波动或监管问询，责任应由软件提供商、审计师还是被审计单位承担？算法偏见问题也值得关注，某些模型可能对特定行业、特定规模的企业系统性误判率更高，但目前没有强制性的算法审计与公平性评估制度。这些规范缺失使得会计师事务所部署智能审计时顾虑重重。

5 研究结论与展望

聚焦财务舞弊识别场景，系统构建了“事前预防-事中监控-事后核查”的智能审计应用框架，通过整合RPA、NLP、北斗定位、知识图谱与机器学习等技术，对虚增收入、存货造假、资金体外循环等典型舞弊模式展开场景化分析，揭示了智能审计在财务舞弊识别中的作用机制与实践效能。研究表明，相较于传统抽样审计，智能审计能够实现从“经验判断”到“数据驱动”、从“事后追溯”到“实时预警”、从“局部抽查”到“全量覆盖”的模式升级。

然而,智能审计在财务舞弊识别的落地过程中,仍面临多重现实约束:①数据层面,舞弊企业的人为数据篡改、多源异构数据孤岛与“垃圾进、垃圾出”效应,制约了模型识别的精准性;②技术层面,浅层规则引擎难以应对复杂舞弊逻辑,而深度学习模型的“黑箱”特性又无法满足审计工作的可解释性要求;③人才层面,审计与数据科学的复合型人才供给不足,人机协同机制尚未成熟,存在过度依赖或抵触技术的双重偏差;④制度层面,针对智能审计的技术标准、数据合规与算法责任界定仍存在监管空白,制约了其在法定审计场景中的规模化应用。

总体而言,智能审计是破解财务舞弊识别难题的关键路径,但其效能的充分发挥,必须建立在“可信数据、可解释技术、复合型人才与完善制度”的协同支撑之上。未来研究可从以下方向深化:①构建面向舞弊场景的专用智能审计模型,强化不同舞弊手段与技术工具的对应关系研究;②探索大模型、数字孪生等前沿技术在舞弊识别中的具体应用路径,提升模型的可解释性与场景适配性;③完善智能审计的监管框架与数据合规制度,明确算法责任与隐私保护边界,推动智能审计与审计准则、监管要求的深度适配,从而全面提升财务舞弊识别的精准性、时效性与权威性,为资本市场高质量发展提供审计监督保障。

参考文献

[1] 陈靖,赵彦. 财务舞弊的手段特征和审计分析应对[J]. 中国注册会计师,2025(1):106-107.

[2] 杨小虎,杨敬懿. AI驱动的舞弊审计系统构建:体系框架与实施路径[J]. 中国注册会计师,2026(2):45-51.

[3] GREENMAN C, ESPLIN D, JOHNSTON R. An analysis of the impact of artificial intelligence on the accounting profession[J]. Journal of Accounting, Ethics & Public Policy, 2024, 25(2): 188.

[4] PAN W. Application and exploration of artificial intelligence technology in audit risk identification[J]. Journal of Social Science and Humanities, 2025, 7(10): 58-61.

[5] LIN Q. Opportunities and challenges of the application of artificial intelligence in the field of auditing[J]. Journal of Innovation and Development, 2025, 13(1): 346-351.

[6] 秦荣生. 大数据、云计算技术对审计的影响研究[J]. 审计研究,2014(6):23-28.

[7] 龙志能,鲍镕江,何贤杰. 人工智能驱动的审计变革研究[J]. 审计研究,2024(5):53-61.

[8] 戚啸艳,王晗,赵洋洋. 人工智能审计的伦理问题及对策研究[J]. 中国注册会计师,2022(6):68-71.

[9] 邓亦玮,韩阳,冉秀娟. 人工智能技术发展与审计创新[J]. 财会月刊,2025(S1):96-105.

[10] 杨寅. 人工智能对审计工作的影响:演进逻辑与分析框架[J]. 财会月刊,2024(18):52-57.

[11] 吴勇,郭秋梦,丁晓月,等. AI技术的审计应用:现状、挑战与应对[J]. 中国注册会计师,2025(11):95-102.

[12] 王雪冰,刘慧. 基于GONE理论的财务舞弊分析:以R公司为例[J]. 老字号品牌营销,2026(2):158-160.

[13] 刘钊,郭小玲,丘书豪. 基于人工智能大模型的企业审计画像数据治理体系探索[J]. 中国内部审计,2025(4):28-35.

[14] 杨萍萍,王凌智,侯彪,等. 基于人工智能的舞弊审计程序优化研究[J]. 会计之友,2025(S2):42-49.

Application of Intelligent Audit Technology in Financial Fraud Identification

WANG Jinhong, YANG Huanyun

(School of Business, Liaocheng University, Liaocheng 252000, China)

Abstract: The increasingly concealed and complicated financial fraud tactics have posed severe challenges to the identification capability and efficiency of traditional auditing. Leveraging its strengths in data processing and analysis, intelligent auditing technology offers a novel solution to the dilemma of financial fraud detection. Based on the GONE(greed, opportunity, need, and exposure) fraud theory, a whole-process intelligent auditing application framework featuring “pre-event prevention, in-process monitoring and post-event verification” was constructed for financial fraud identification. Technologies including robotic process automation(RPA), natural language processing(NLP), Beidou positioning system, knowledge graph and machine learning were systematically integrated. Scenario-specific analyses were conducted on typical financial fraud cases including revenue overstatement, inventory fraud and off-balance sheet capital circulation. It is indicated that intelligent auditing drives the transformation of auditing models: shifting from sampling auditing to full-volume auditing, from empirical judgment to data-driven decision-making, and from post-event traceability to the integration of pre-event prevention and in-process monitoring. Additionally, practical dilemmas in the application of intelligent auditing for fraud identification were further explored. Theoretical support and practical references are provided for the compliant and large-scale application of intelligent auditing in financial fraud identification, so as to enhance the efficiency of audit supervision in the capital market.

Keywords: intelligent audit; financial fraud; risk prevention and control; GONE(greed, opportunity, need, and exposure) fraud theory