

doi: 10.7690/bgzd.2025.10.004

基于深度学习的电子发票异常行为检测模型

王 岩, 黄 莹, 郭 威

(海南电网有限责任公司信息通信分公司, 海口 570203)

摘要: 针对电子发票流通过程中产生的异常行为趋于多样化和复杂化等特点, 提出一种基于深度学习的电子发票异常行为检测模型。对用户消费中某些敏感信息进行加工并聚类处理, 建立异常行为特征数据集; 提出一种结合双线性投影及注意机制的深度网络学习企业消费数据, 并在网络中引入注意增强双线性层(bilinear layer, BL)模型, 提高模型训练效率; 以某财务公司提供的企业开具发票行为数据为例, 对所提检测模型的有效性进行验证。结果表明: 所提模型性能最高, 平均识别准确率为 93.25%; 与 ResNet、VGG 和 LSTM 模型相比, 准确率分别提升 6.6%、6.42%和 5.27%。

关键词: 财务; 电子发票; 深度学习; 异常分析; 双线性投影; 注意机制

中图分类号: TP393 **文献标志码:** A

Abnormal Behavior Detection Model of Electronic Invoice Based on Deep Learning

Wang Yan, Huang Ying, Guo Wei

(Information and Communication Branch of Hainan Power Grid, Haikou 570203, China)

Abstract: In view of the characteristics that the abnormal behaviors generated in the circulation of electronic invoices tend to be diversified and complicated, this paper proposes an electronic invoice abnormal behavior detection model based on deep learning. Some sensitive information in user consumption is processed and clustered to establish a data set of abnormal behavior characteristics. A deep network learning enterprise consumption data combined with bilinear projection and attention mechanism is proposed, and an attention-enhanced bilinear layer (BL) model is introduced into the network to improve the training efficiency of the model. The validity of the proposed detection model is verified by the data of enterprise invoicing behavior provided by a financial company. The results show that the proposed model has the highest performance, and the average recognition accuracy is 93.25%; compared with ResNet, VGG and LSTM models, the accuracy is improved by 6.6%, 6.42% and 5.27%, respectively.

Keywords: finance; electronic invoice; deep learning; anomaly analysis; bilinear projection; attention mechanism

0 引言

计算机、网络、大数据、物联网、通信等技术^[1-2]的不断发展为智能财务^[3-5]的改革与创新带来了契机。目前, 电子发票^[6]在企业中得到广泛应用, 并逐渐取代传统的纸质发票, 成为报销和纳税的重要凭证。电子发票的生命周期包括签发、储存、验证、报销等过程, 在这个过程中, 可能会出现电子发票超限/类型签发、重复/虚假发票报销、虚假系统连接等异常行为。为保证电子发票系统的正常运行, 需要对上述异常情况进行严格监管。

为此, 大量学者对电子发票系统进行了研究, 并取得了丰硕成果。文献[7]从理论和实践层面分析了建筑施工企业的异常发票问题, 提出了建筑施工企业异常发票风险控制策略。文献[8]基于随机森林算法对企业的进销项发票数据进行分析, 并建立企业税收风险的预测模型, 从而提高国家有关机关稽

查企业异常发票问题。文献[9]提出一种基于签名认证的、验证电子发票真伪的可行性方案, 通过对税务机构签名进行验证, 检验空白电子发票是否具有合法性。目前, 应用于电子发票系统的异常行为自动检测的相关文献较少: 一方面, 单张发票中的异常行为可以在终端通过简单的研究和判断来实现, 但是对于大量用户异常行为(如虚开发票)产生的数据, 目前还没有明确的分析方法; 另一方面, 电子发票流通过程中产生的异常行为是多样的、多变的, 传统的统计方法对海量异常数据的分析过于局限, 无法在异常行为数据中挖掘用户与企业之间的潜在联系。针对上述问题, 笔者提出一种基于深度学习的电子发票异常行为判断方法。

1 模型结构

图 1 为基于深度学习的电子发票异常行为检测

收稿日期: 2024-10-07; 修回日期: 2024-11-08

第一作者: 王 岩(1995—), 女, 陕西人。

模型。该模型分为：隐私保护、特征提取、模型训练和异常行为检测 4 个模块，可实现对短时间内开具大量发票、短时间内开具大量大额发票、非正常时间内开具大量发票、非正常时间内开具大量大额发票 4 种异常行为的准确研究和判断。

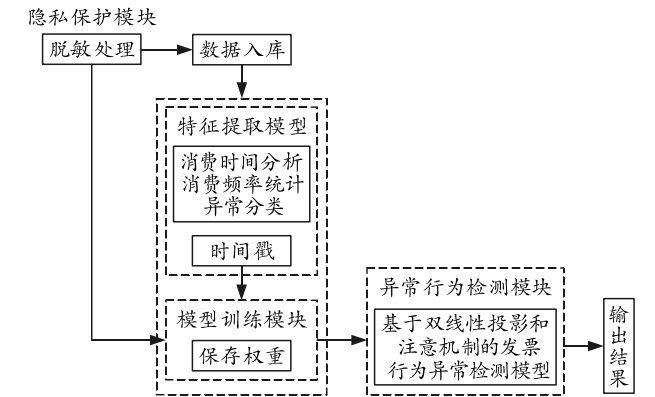


图 1 基于深度学习的电子发票异常行为检测模型

1) 隐私保护模块会降低所有用户隐私数据的敏感度。

2) 特征提取模块包括：数据读取单元和数据处理单元。数据读取单元负责读取数据库中的历史电子发票数据和企业正常开具的发票期间数据。数据处理单元由消费时间分析、消费频率统计和异常分类 3 部分组成。消费时间是将读取的电子发票数据中的时间信息与企业的正常消费周期进行比较，以确定每一条数据是否由企业在正常消费周期内发出；统计消费频率是分别对正常时段和异常时段的数据进行处理，提取 2 种数据在固定时段的消费量，并在相应的数据上进行标记；异常数据分类是对统计消费频率后的数据进行聚类分析，根据聚类结果判断读取的数据是否为异常数据，并对异常数据进行标记。

3) 模型训练模块将上述特征数据输入到深度学习模型中进行训练，模型的输入采用数据处理单元提取的特征值，最终保存训练权重。

4) 异常行为检测模块可根据预训练的模型权重输出分类结果，从而实现基于输入数据对异常行为进行智能分析和判断。需注意，电子发票异常行为检测模型可定期读取数据库中的新数据，然后将处理后的数据输入到深度学习模型继续训练，从而进一步更新权重，实现模型迭代优化过程。

2 关键技术

2.1 用户隐私数据保护

用户隐私数据保护是指通过脱敏规则对用户某

些敏感信息进行加工，以实现用户敏感隐私数据的可靠保护。笔者使用的企业消费数据包含用户个人信息和企业信息等敏感数据，因此笔者在数据处理和分析之前对用户敏感信息进行了脱敏处理。使用的数据包含可识别数据序列，如发票号、用户 ID 和企业 ID，数据部分字段信息如表 1 所示。上述 2 个可识别列的数据用字符替换，同时需保证替换的字符与之前的字符可一一对应。

表 1 数据部分字段信息

序号	描述	序号	描述
1	企业 ID	4	开票数量
2	用户 ID	5	开票金额
3	开票时间		

2.2 特征提取

根据实际情况，非法发票等异常消费情况通常在较短时间内完成，具有集中化的特点。为此，根据每条数据的消费时间是否在正常消费时段(如正常消费时段 8:00 至 22:00；异常消费时段 22:00 至第 2 日凌晨 8:00)，可将数据信息分为正常消费时段数据和异常消费时段数据 2 类。对于每种类型的数据信息，将时间信号从短信转换为时间戳，在固定时间内抽取同一企业的发票数量并进行分析，可以有效地描述开具发票的 4 种异常行为特征。主要异常行为分 4 种类型：1) 公司在短时间内开具大量发票(事件 1)；2) 公司在短时间内开具了大量大额发票(事件 2)；3) 公司在非正常时间开具大量发票(事件 3)；4) 公司在非正常时间(事件 4)开具一张大额发票。

2.3 发票行为异常检测模型

提出一种结合双线性投影及注意机制的深度网络学习企业消费数据，并将注意增强双线性层(BL)模型引入网络中，让模型能够采取所有的小批量梯度下降学习算法，开展相应的训练。

2.3.1 双线性层

令 $X=[x_1,x_2,\cdots,x_T]\in\mathbb{R}^{D\times T}$ 表示 BL 的输入。按照双线性映射回归模型，BL 层会借助下列映射，对大小达到了 $D\times T$ 的相关输入进行转换，使其变成大小达到了 $D'\times T'$ 的矩阵：

$$Y=\phi(W_1XW_2+B)。(1)$$

式中： $W_1\in\mathbb{R}^{D\times D'}$ 、 $W_2\in\mathbb{R}^{T\times T'}$ 、 $B\in\mathbb{R}^{D'\times T'}$ 为需要估计的相关参数； $\phi(\bullet)$ 为 sigmoid 或者 ReLU 这样的元素

非线性变换函数。

值得注意的是，估计参数的个数与每个输入模式的维数成线性关系，而不是与输入神经元的个数成线性关系。对于多层感知器 (multilayer perceptron, MLP) 层，将 $D \times T$ 大小的输入转换为 $D' \times T'$ 要预测 $(DT+1)D'T'$ 个参数 (涵盖偏置项)，极大地超过了 BL 本身的参数数目 ($DD'+TT'+D'T'$)。

进一步，将映射应用于时间序列数据时，一个更重要的特征是，BL 建立了 2 个依赖项 (输入表示的每个模式)，且每个依赖项具有不同的语义。为了更好地理解这一点，将 X 的每列和每行分别表示为 $x_{c_t} \in \mathbb{R}^D$, $t=1, 2, \dots, T$ 和 $x_{r_d} \in \mathbb{R}^D$, $d=1, 2, \dots, D$ 。在输入时间序列 X 给定的情况下，第 t 列为在时间实例 t 处能够看到的不同特征达到了 D 个，第 d 行涵盖了过去 t 个步骤过去中第 d 个特征出现的时间变化；因此，有：

$$W_1 X = [W_1 x_{c_1}, W_1 x_{c_2}, \dots, W_1 x_{c_T}] ; \quad (2)$$

$$X W_2 = \begin{bmatrix} (x_{r_1})^T W_2 \\ \vdots \\ (x_{r_D})^T W_2 \end{bmatrix} . \quad (3)$$

式中： $W_1 X$ 为在时间实例 $t=1, 2, \dots, T$ 时各种特征间的彼此作用，通过 W_1 反映出来； W_2 为第 d 个特征的相关时间进程。如果 X 涵盖历史 T 期间 LOB 水平不同的 D 个股票价格，BL 借助 W_1 明确在特定时间不同股票价格如何彼此作用的情况，借助 W_2 明确特定指数的相关价格究竟如何随着时间推移而变化；所以，采取 LOB 中的相关空间结构，能够对今后最合适的买卖价格做出更有效的联合分配。

2.3.2 时间注意增强 BL 模型

虽然 BL 可以按照各特征对独立的依赖关系进行学习，然而不明确某个时间实例的相关表示怎么样和其他时间实例进行交互，或哪些时间实例在预测视界 T' 处能够起到至关重要的作用。笔者在注意力计算方案中融入位置信息，学习模型只采取过去序列中的相关特定时间实例对给定视界下的相关未来值进行预测，对序列间学习非常有利。时间注意增强 BL 模型 (映射输入 $X \in \mathbb{R}^{D \times T}$ 到输出 $Y \in \mathbb{R}^{D' \times T'}$) 被提出来：

$$\bar{X} = W_1 X ; \quad (4)$$

$$E = \bar{X} W ; \quad (5)$$

$$\alpha_{ij} = \exp(e_{ij}) / \sum_{k=1}^T \exp(e_{ik}) ; \quad (6)$$

$$\tilde{X} = \lambda(\tilde{X} \odot A) + (1-\lambda)\bar{X} ; \quad (7)$$

$$Y = \phi(\tilde{X} W_2 + B) . \quad (8)$$

式中： α_{ij} 、 e_{ij} 依次为 A 和 E 位置 (i, j) 处的相关元素； $\odot$ 为多重复制元素级算子； $\phi(\cdot)$ 为预定义的一个非线性映射，如式 (1) 所示； $W_1 \in \mathbb{R}^{D' \times D}$ 、 $W \in \mathbb{R}^{T \times T}$ 、 $W_2 \in \mathbb{R}^{T \times T'}$ 、 $B \in \mathbb{R}^{D' \times T'}$ 、 λ 为所提注意增强 BL 模型的参数。类似于前文所述的基础 BL 模型，注意增强 BL 模型采取 W_1 、 W_2 打造了彼此独立运行的依赖模型，而且借助 W 、 λ 对中间注意过程进行学习。

注意增强 BL 模型流程如图 2 所示，涵盖了 5 个具体步骤。

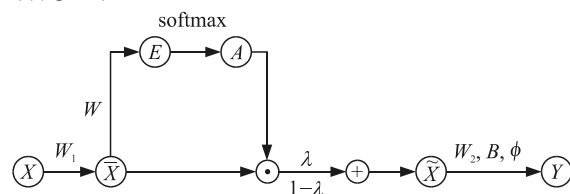


图 2 注意增强 BL 模型流程

步骤 1 按照式 (4)， W_1 把 X (每列) 的各时间实例 x_{c_t} , $t=1, 2, \dots, T$ 的表示转换为另外的特征空间 $\mathbb{R}^{D'}$ 。该模型依据 X 的首个模式形成依赖关系，而且使时间顺序保持最初的模样。

步骤 2 深入探讨对角线元素固定为 $1/T$ 的结构矩阵 W 的相关内容。令 $\bar{x}_t \in \mathbb{R}^{D'}$ 、 $e_t \in \mathbb{R}^{D'}$ 分别代表 $\bar{X}$ 、 E 的第 t 列。结合式 (5) 能够看出， e_t 是在特征空间 $\mathbb{R}^{D'}$ 内数量达到 T 个的时态实例的相应加权组合。从 $\bar{X}$ 的 T 列来看，因为 W 拥有固定为 $1/T$ 的对角线元素，所以第 t 个时间实例的相应权重一直都是 $1/T$ 。在这种情况下， E 中的 e_{ij} 对编码比较关键的元素 x_{ij} 进行编码，但 $\bar{x}_{ik}$, $k \neq j$ 却被忽略了。

步骤 3 采取式 (6) 的 softmax 函数，归一化处理 E 中的相关重要值。这一层推动不少元素趋近于 0 的位置，而且要保持少部分元素的值为正。在此环节中会形成注意力掩码 A 。

步骤 4 从上一步骤获得的注意掩码 A 可以将 $\mathbb{R}^{D'}$ 中无关紧要元素的影响消除掉。在式 (7) 中， λ 允许模型能够对软注意机制进行学习，不再学习过去的硬注意机制。鉴于在早期的学习过程中，可能从前一层提取的学习特征中有噪声，硬注意机制会误导模型到非关键信息上面，但软注意机制会先学习相关的辨别特征，再让模型选择最关键的那些特

征。应该指出的是, λ 的取值范围是 $[0, 1]$ 。

步骤 5 类似于 BL 模型, 最后是对时间映射 W_2 进行估算, 在非线性变换以及偏置后能够将级别更高的特征提取出来。

通常情况下, 注意增强 BL 模型的步骤 2—4, 可以采取注意机制, 对代表相同特征的不同时间步的神经元间的竞争产生激励作用, 也就是说, 对 $\bar{X}$ 的同一行上的相关元素而言, 相互之间会进行更大的竞争。针对 $\mathbb{R}^D$ 中的各特征, 也就是说对 $\bar{X}$ 同一列的相关元素而言, 这种竞争又处于独立的态势。

2.3.3 网络结构

如图 3 所示是网络结构。输入矩阵的大小达到了 $M \times N$, 其中 M 表示特征数, N 表示异常事件数。虽然注意机制可以放在任何一层, 但该过程类似于应用多个卷积层后应用的视觉注意机制, 所以笔者认为, 网络参与高级表征更为有利。而且, 鉴于评估的网络结构输出就是隶属度概率向量, 所以采取加权熵损失函数评价相关结果:

$$L = -\sum_{i=1}^3 \frac{c}{N_i} y_i \log(\tilde{y}_i) \quad (9)$$

式中: $\tilde{y}_i$ 、 y_i 、 N_i 依次为第 i 类的预测概率、真实概率以及样本数; c 为常数, 可规避损失值除以 N_i 时非常小的情况, 以保障数值具有稳定性。

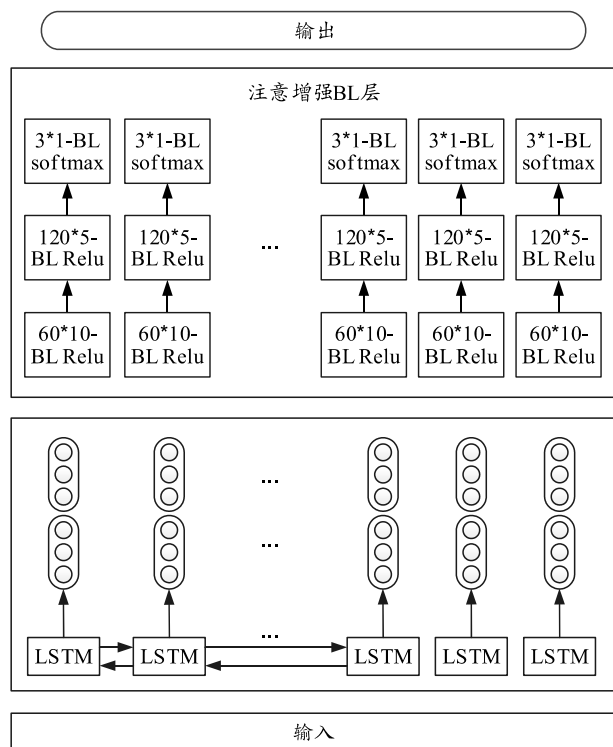


图 3 网络结构

3 仿真与分析

3.1 数据集与环境设置

笔者基于某财务公司提供的企业开具发票行为数据并构成异常行为数据集。为保护用户及企业隐私, 对发票号、用户 ID 和企业 ID 等进行脱敏处理。对选定数据样本进行分类并剔除异常值, 最终数据集中包含 120 个公司, 涉及新能源、制造、电信、互联网、通信 5 大领域, 共包含 62 230 条数据。

仿真时软件环境为: Ubuntu 18.04 操作系统, 深度学习网络模型由 TensorFlow 和 keras 深度学习框架搭建, 编程语言为 Python; 硬件环境为: 联想 P700 服务器 (CPU 型号 Xeon e5-2640 v3, 64 GB 内存, 2 T 硬盘, 配备 NVIDIA RTX2080TiGPU)。

3.2 训练与评估

数据集被划分成了测试集、验证集和训练集 3 部分, 比例大小为 2:1:7。网络训练时输出学习率设置为 0.000 1, 学习率衰减倍数设置为 0.1, 批处理大小设置为 16, 最大迭代步长设置为 150。同时, 为避免过拟合, 深度网络中采用了 dropout 策略, 且概率设置为 0.16。LSTM 的隐藏层和隐藏层节点数分别设置为 2 和 128。

图 4 为所提模型的相应性能曲线。该模型采取了传统意义上的交叉熵损失函数与笔者所提损失函数开展相应训练, 在训练过程中开始迭代。可以看出: 损失函数训练的相关模型使用本文中方法, 大概在 30 代的情况下大致能够实现最优迭代, 但传统意义上的交叉熵损失大致在 100 代的情况下才可以得到最优迭代。可见, 相比于传统交叉熵损失所提的相关损失函数的训练效率提升 2.33 倍。

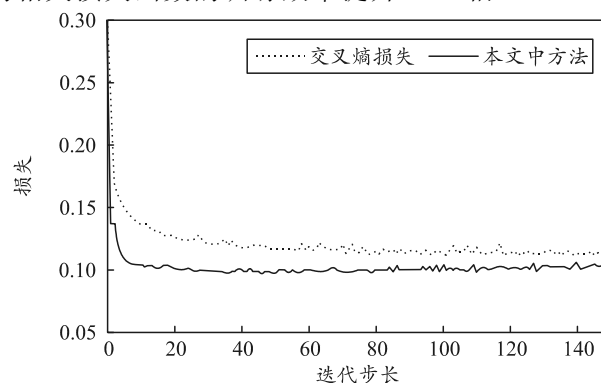


图 4 不同损失函数仿真对比结果

3.3 不同模型对比分析

将所提双线性投影和注意机制的发票行为异常检测模型与人工神经网络 (artificial neural network,

ANN)^[10]、支持向量机 (support vector machine, SVM)^[11]、ResNet52^[12]、VGG^[13]、长短期记忆网络 (long short term memory, LSTM)^[14]等方法进行对比实验,不同模型准确率、召回率和 F_1 分数对比结果如表 2 所示。

表 2 平均准确率比较结果

模型	准确率/%	召回率/%	F_1 分数
SVM	76.33	68.42	72.16
神经网络(隐含层为 20)	80.21	78.54	79.37
ResNet52	86.65	80.14	82.33
VGG19	86.83	82.31	84.51
LSTM(隐藏层 2 和隐藏层节点数 128)	87.98	81.35	84.54
所提模型	93.25	89.67	91.43

由表 2 可以看出: SVM 和 ANN 性能最低,识别准确率仅为 76.33%和 80.21%; ResNet52 和 VGG 模型性能有所提升,分别为 86.65%和 86.83%; LSTM 模型性能较 ResNet52 和 VGG 提升不明显,识别准确率为 86.83%; 所提模型性能最高,平均识别准确率为 93.25%。与 ResNet、VGG 和 LSTM 模型相比,所提模型准确率分别提升 6.6%、6.42%和 5.27%。实验结果表明,所提模型可以有效识别异常开票行为。

4 结论

笔者基于深度学习模型对企业异常开票行为进行分析,提出一种基于深度学习的电子发票系统异常检测模型。模型分为隐私保护、特征提取、深度学习训练和异常行为检测模块,可实现企业短时间内开具大量发票、短时间内开具大量大额发票、非正常时间内开具大量发票、非正常时间内开具大量大额发票 4 种异常行为的识别和判断。未来,引入开票机器 IP 地址、开票种类等提供特征信息,从而进一步提升模型可识别异常发票的种类。所提基于深度学习的电子发票系统异常检测模型可用于企业财务自动监测,为智能化财务管理提供一定借鉴

作用。

参考文献:

- [1] 毛龙灿, 杨南. 基于大数据背景的皮革人才培养优化研究[J]. 中国皮革, 2021, 50(9): 38-41.
- [2] 杨涛. 互联网时代下皮革行业电商物流体系研究分析[J]. 中国皮革, 2021, 50(8): 82-85.
- [3] 姜雅楠. 大数据时代下会计信息化的风险因素及防范措施[J]. 办公自动化, 2022, 27(4): 53-55.
- [4] 杨晶. “互联网+”人工智能下高校财务报账新模式探究[J]. 纳税, 2021, 15(36): 89-91.
- [5] 黄坚, 牟晓霞, 李晓英. 智能财务对企业数字化转型作用研究[J]. 企业科技与发展, 2021(12): 140-142.
- [6] 陈寰, 袁小丽. 电子发票管理的涉税风险及对策[J]. 湖南税务高等专科学校学报, 2022, 35(1): 68-71.
- [7] 张春林. 建筑施工企业异常发票风险控制研究[J]. 会计师, 2021(22): 118-119.
- [8] 孔丽英, 林晓玲, 吴铮涛, 等. 基于企业进销项发票数据的税收风险预测模型[J]. 肇庆学院学报, 2020, 41(2): 1-8.
- [9] 谢绒娜, 毛卫华, 史国振. 基于签名认证的电子发票真伪性验证方案[J]. 网络与信息安全学报, 2019, 5(6): 105-112.
- [10] 李钰, 刘莉, 吕会影. 支持向量机和人工神经网络在期权价格预测中的比较研究[J]. 西昌学院学报(自然科学版), 2022, 36(2): 31-36.
- [11] 黄为新, 陶杨, 张继超, 等. 基于迁移学习的发票号码识别研究[J]. 软件导刊, 2021, 20(6): 45-48.
- [12] 陈勇, 党淑雯, 聂铃. 基于 ResNet 模型的回环检测算法[J]. 智能计算机与应用, 2022, 12(8): 196-199.
- [13] 孙凯文, 陶建峰, 谷朝臣, 等. 基于改进 VGG16 网络的 TBM 围岩识别方法研究[J]. 自动化仪表, 2022, 43(7): 6-11, 16.
- [14] 王佳钰, 郝思鹏, 李森文, 等. 基于 ES-GRU-LSTM 的风电场群功率预测[J]. 计算技术与自动化, 2022, 41(3): 37-41.