融合自适应 SSAE 与神经网络算法的区块链隐私保护模型研究

刘伟伟 [1]
LIU Weiwei

摘 要 针对区块链隐私保护与审计追溯的难题，研究对基于自适应堆叠稀疏自编码器与神经网络算法的区块链隐私保护模型进行了研究。采用灰狼优化算法（grey wolf optimization algorithm, GWO）的关键技术，对自适应堆叠稀疏自编码器进行改进，并结合支持向量机实现数据敏感度的精准识别与差异化加密策略。经实验测试实现了恶意行为的低封锁时间，最高峰值仅为 1.1 ms，但整体波动较大。该模型在区块链隐私保护分类任务中准确率达到 95.01%，F_1 分数为 94.23%，召回率为 93.45%，精确率为 95.66%。模型展现出了良好的抗干扰能力和稳定性，尤其在处理高度敏感信息时表现突出，有效提升了区块链系统的隐私保护水平。

关键词 堆叠稀疏自编码器（SSAE）；区块链；隐私保护；灰狼优化算法（GWO）

doi：10.3969/j.issn.1672-9528.2025.10.009

0 引言

随着区块链技术的快速发展，其在提供去中心化、安全数据存储的同时，也面临着用户隐私泄露的风险 [1-2]。当前，区块链在供应链等领域的应用愈发广泛，对隐私保护与审计追溯的需求日益迫切 [3-4]。吴勐 [5] 提出基于有向图和零知识证明的隐私保护模型。结果显示，该方法以轻微吞吐量代价实现了完整审计与追溯。Devidas 等人 [6] 提出了一种身份可验证的环签名方案。结果显示，该方案能有效保护隐私并确定真实签名者。相关研究虽提出基于区块链的隐私保护模型，但却未全面考虑数据完整性和共识效率 [7-8]。鉴于此，本研究创新性地提出了融合自适应堆叠稀疏自编码器与神经网络算法的区块链隐私保护模型（blockchain with self-adaptive stacked sparse autoencoder-neural network privacy protection, BSSA-NNPP），通过分类算法实现数据敏感度的精准识别与差异化加密。研究旨在解决区块链隐私保护中的数据分类不准确、加密策略单一及共识机制效率低下等问题，为区块链技术在数据共享与隐私保护领域的应用提供新的思路。

1 BSSA-NNPP 区块链隐私保护方案总体设计

区块链隐私保护模型需确保数据在不同敏感度级别下得到恰当保护 [9-10]。分类算法通过分析数据重要性及泄漏风险，帮助选择恰当的加密方式 [11-12]。因此，研究引入分类算法来制定差异化的加密策略。研究提出的 BSSA-NNPP 区块链隐私保护模型主要包含了 5 大功能模块。数据预处理模块利用数据清洗算法和 Python 的 Pandas 库，负责收集、清洗和标准化区块链中的庞杂原始数据。数据敏感度分类模块采用自适应堆叠稀疏自编码器（adaptive stacking of a sparse auto encoder, ASSAE）算法。加密策略决策模块根据数据敏感度分类的结果，选择合适的加密策略，并指导数据加密执行模块进行加密操作。数据加密执行模块执行加密策略决策模块的指令，利用 OpenSSL 库等加密算法实现对区块链数据的实际加密操作。数据访问控制模块根据数据的敏感度级别和用户的访问权限，严格控制对区块链数据的访问。

2 ASSAE-GWO-SVM 分类算法设计

在 BSSA-NNPP 方案中，数据敏感度分类模块是重要部分。堆叠稀疏自编码器（SSAE）通过计算自编码的输出与原输入的误差，不断调节自编码器的参数 [13-14]。为了更好地适应区块链隐私保护对数据安全性、高效性和适应性的高要求，研究采用 Dropout 机制代替 KL 散度，并引入灰狼优化算法（grey wolf optimization algorithm, GWO）进行自适应网络参数寻优，改进后的 ASSAE 结构示意图如图 1 所示。

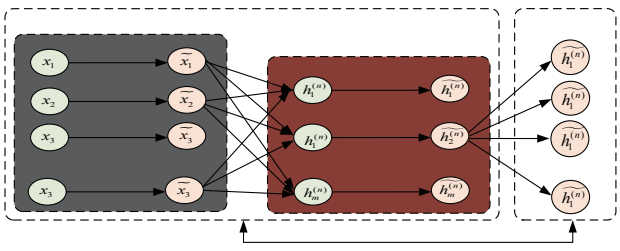

图 1 ASSAR 结构示意图

1. 山西电子科技学院 山西临汾 041000

图 1 清晰地描绘了编码层、解码层以及 Dropout 层的布局与功能。在传统 SSAE 中，KL 散度常被用作稀疏约束，但这种方法容易导致过拟合，并且网络结构参数的设置往往依赖于人工经验，需要大量重复实验，不仅耗时费力，而且结果具有不稳定性。为了克服这些局限，ASSAR 采用了 Dropout 机制代替 KL 散度进行稀疏约束。当 ASSAR 采用 Dropout 机制，则该网络可以描述为：

$$\begin{cases} r_j^{(l)} \sim \text{Bernoulli}(p) \\ \tilde{\boldsymbol{y}}^{(l)} = \boldsymbol{r}^{(l)} \cdot \boldsymbol{y}^{(l)} \\ \boldsymbol{z}_i^{(l+1)} = \boldsymbol{W}_i^{(l+1)} \tilde{\boldsymbol{y}}^{l} + \boldsymbol{b}_i^{(l+1)} \\ \boldsymbol{y}_i^{(l+1)} = f\left(\boldsymbol{z}_i^{(l+1)}\right) \end{cases} \tag{1}$$

式中：$r_j^{(l)}$表示第 l 层的第 j 个神经元是否被保留的伯努利随机变量，其取值范围为 0 或 1；$\tilde{\boldsymbol{y}}^{(l)}$表示第 l 层的输出在经过 Dropout 处理后的值，是原始输出$\boldsymbol{y}^{(l)}$与随机向量 $\boldsymbol{r}^{(l)}$ 的逐元素乘积；$\boldsymbol{z}_i^{(l+1)}$表示第 l+1 层的输入值，是第 l 层 Dropout 处理后的输出$\tilde{\boldsymbol{y}}^{l}$与权重$\boldsymbol{W}_i^{(l+1)}$的矩阵乘积加上偏置$\boldsymbol{b}_i^{(l+1)}$；$\boldsymbol{y}_i^{(l+1)}$表示第 l+1 层的输出值，是激活函数 f 应用于$\boldsymbol{z}_i^{(l+1)}$的结果。

Dropout 机制通过在训练过程中随机丢弃神经网络中的单元及其连接，从而显著减少了过拟合现象。此外，ASSAR 还引入了 GWO 进行网络参数自适应寻优。假设用 n_l 表示 MSSAE 第 n 层的神经元个数。希望找到一组最优的神经元个数，使得网络在训练集上的某种性能指标达到最优，同时满足稀疏性约束等条件。这个过程的目标函数用公式表示为：

$$\begin{cases} \min\limits_{\theta} J(\theta) = L(\boldsymbol{y}_L, \hat{y}) + \lambda R(\theta) + \gamma C(\theta) \\ \text{s.t. } \boldsymbol{z}_l = m_l \odot \boldsymbol{y}_l, \quad m_l \sim \text{Bernoulli}(p_l), \quad l = 1,2,\ldots,L \\ \boldsymbol{y}_l = f_l(\boldsymbol{W}_l s_{l-1} + \boldsymbol{b}_l), \quad l = 1,2,\ldots,L \\ n_l \in \boldsymbol{Z}^+, \quad l = 1,2,\ldots,L \end{cases} \tag{2}$$

式中：$\boldsymbol{y}_L$ 为第 l 层的输出值（在应用激活函数之前）；$\boldsymbol{s}_l$ 为第 l 层应用 Dropout 之后的输出值；f_l 为第 l 层的激活函数；p_l 为第 l 层 Dropout 的保留概率；$L(\cdot)$ 为损失函数；λ 为正则化系数；$R(\cdot)$ 为正则化项（如 L2 正则化）；θ 为网络的所有参数（包括 n_l、$\boldsymbol{W}_l$、$\boldsymbol{b}_l$ 等）；$C(\theta)$ 为稀疏性约束（如限制神经元的平均激活度）。

通过算法寻优，ASSAE 能够自动确定每一层的神经元个数，从而消除了传统 SSAE 中参数设置的不稳定性，并减少了网络计算量。再利用 ASSAE 进行特征提取之后，研究引入了支持向量机对特征进行分类处理，最终构建出一种新的数据敏感分类算法（ASSAE-GWO-SVM），其结构示意图如图 2 所示。首先，训练集数据被输入到 ASSAE 中逐层提取特征。每一层都通过重构误差进行训练，并应用 Dropout 技术增强泛化能力。然后，ASSAE 中的编码器和解码器共同进行特征提取。接着，引入 GWO 算法进行网络参数自适应寻优，使得网络的性能指标达到最优，同时满足约束条件。随后，利用训练好的 ASSAE 进行特征提取，并将提取的特征输入到支持向量机中进行分类处理。此外，GWO 模块也被用来优化 SVM 参数。在构建 SVM 模型时，系统会检查序列检测是否为全局最优，一旦确认全局最优，将利用支持向量进行 SVM 训练，最终构建 ASSAE-GWO-SVM 分类模型。

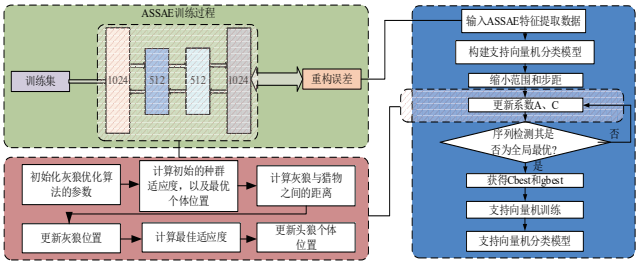

图 2 ASSAE-GWO-SVM 分类算法结构示意图

3 BSSA-NNPP 性能分析与应用性实验

为了对区块链高度敏感信息进行分类处理，研究设计出一种 ASSAE-GWO-SVM 模型，为了验证该模型各个组件的重要性，研究进行了模型消融性实验，并设置了一系列实验组。

组 1：作为基准实验组，使用了标准的 ASSAE-GWO-SVM 模型，没有进行任何额外的优化或改进。

组 2：在基准模型的基础上，增加了 Dropout 机制，设置 Dropout 率为 0.5，以增强模型的泛化能力，减少过拟合现象。

组 3：在组 2 的基础上，引入了 GWO 来自动优化 ASSAE 中每一层的神经元个数，以找到最优的网络结构，提高模型的性能。

组 4：在组 3 的基础上，进一步对 SVM 的参数进行了优化。

组 5：在组 4 的基础上，增加了数据增强技术，对训练集数据进行了旋转和缩放等操作，以增加数据的多样性，提高模型的鲁棒性和泛化能力。实验结果如表 1 所示。

表 1 ASSAE-GWO-SVM 模型消融实验结果表

单位：%

实验组	准确率	F_1 分数	召回率	精确率
组 1	92.34	91.23	90.12	92.34
组 2	93.45	92.56	91.67	93.45
组 3	94.12	93.09	92.34	94.01
组 4	94.67	93.89	92.89	94.68
组 5	95.01	94.23	93.45	95.66

组 1 作为基准实验组，准确率为 92.34%，F_1 分数为 91.23%，召回率为 90.12%，精确率为 92.34%，表现出了良好的基线性能。

组 2 通过增加 Dropout 机制并设置 Dropout 率为 0.5，模型的各项性能指标均有所提升，准确率提高了 1.11 个百分点，F_1 分数、召回率和精确率也分别提升了 1.33、1.55 和 1.11 个百分点，证明了 Dropout 机制在增强模型泛化能力和减少过拟合方面的有效性。

组 3 引入 GWO 后，模型性能进一步提升，准确率达到了 94.12%，相比组 2 提高了 0.67 个百分点，F_1 分数、召回率和精确率也均有提升，这表明 GWO 算法在优化网络结构方面的作用显著。

组 4 在组 3 的基础上进一步优化了 SVM 的参数后，模型性能得到了进一步提升，准确率达到了 94.67%，相比组 2 提高了 0.55%。同时，F_1 分数、召回率和精确率也有所提升。表明优化 SVM 的参数能够有效改善模型的性能。

组 5 通过增加数据增强技术，进一步提高了模型的鲁棒性和泛化能力，准确率达到了最高的 95.01%，精确率也大幅提升至 95.66%，这充分证明了数据增强技术在提升模型性能方面的有效性。

为了验证该 BSSA-NNPP 方案在实际的区块链隐私保护中的分类效果，研究将该模型应用于实际的区块链加密过程，对高度敏感信息、较敏感信息、中等敏感度信息、低敏感度信息、公开信息、系统日志信息、临时数据进行分类处理，为了进一步同时验证该算法的优越性，研究引入了文献 [15] 提出的多监管差分隐私共享模型（multi-regulatory differential privacy-sharing model, MDPSM）进行对比，两种模型分类过程中的混淆矩阵如图 3 所示。

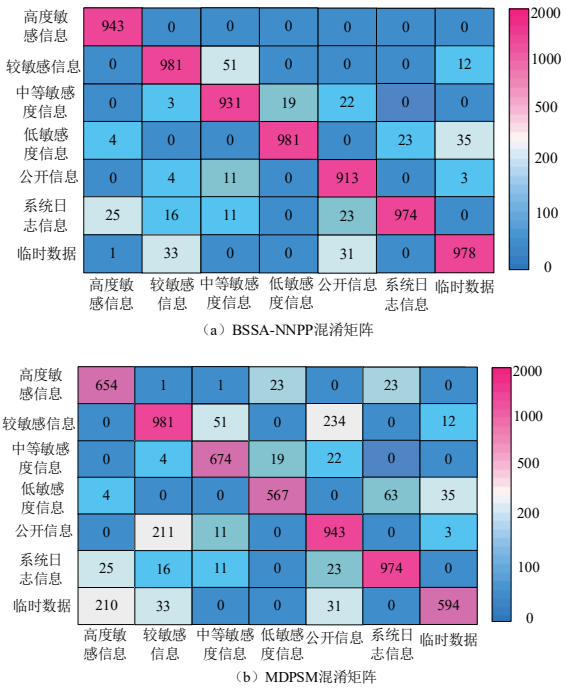

图 3 BSSA-NNPP 分类混淆矩阵

根据图 3 所示的混淆矩阵，BSSA-NNPP 方案在区块链隐私保护分类任务中展现出一定的准确性，但仍存在改进空间。模型在高度敏感信息分类上表现突出，正确分类了 943 个样本。对于较敏感信息，模型同样表现良好，正确分类 981 个，但有 51 个被误判为中等敏感度信息。在中等敏感度信息分类中，模型正确分类 931 个样本，但存在与低敏感度信息和较敏感信息的混淆，分别有 19 个和 22 个误分类。对于低敏感度信息，模型分类效果稍逊，正确分类 981 个，但有 23 个被误判为公开信息，另有 35 个被错误归类到其他类别。与 BSSA-NNPP 方案相比，MDPSM 模型的识别准确率则要差许多。综上所述，BSSA-NNPP 方案在整体分类任务中表现尚可，但应针对低敏感度信息和临时数据的分类进行进一步优化，以减少误分类，提升模型性能。区块链共识机制中包含了多种用户行为，实验测试了不同行为对该 BSSA-NNPP 方案的影响，实验结果如图 4 所示。

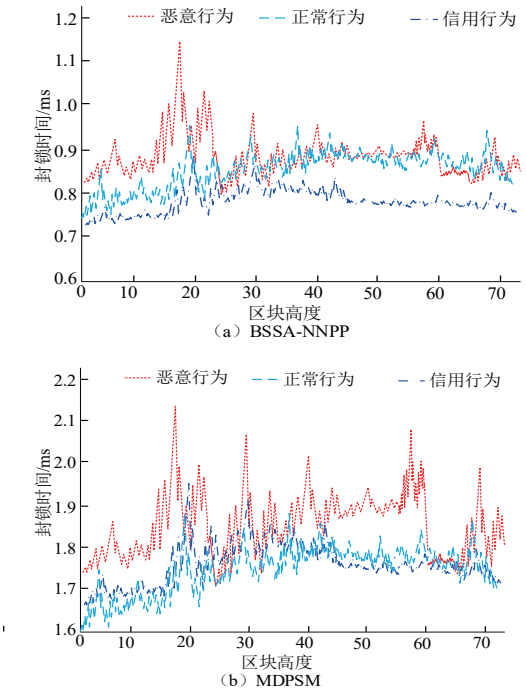

图 4 不同行为对该 BSSA-NNPP 方案的影响

图 4 展示了不同用户行为对 BSSA-NNPP 方案的影响。恶意行为的封锁时间在某些区块高度上显著上升，最高峰值达到约 1.1 ms，但整体波动较大。相比之下，正常行为和信用行为的封锁时间则相对平稳，最高分别约为 0.9 ms 和 0.8 ms。尽管恶意行为在某些区块高度上对系统产生了较大冲击，但 BSSA-NNPP 方案展现出了良好的抗干扰能力。恶意行为的封锁时间虽有波动，但总体维持在 1.2 ms 以内，系统并未因此出现长时间的异常。而 MDPSM 模型的封锁时间，则在 1.6~2.2 ms 之间，大幅高于 BSSA-NNPP 方案。上述结论的原因和机制主要在于 BSSA-NNPP 方案对数据的精细分

类和差异化加密策略。模型通过 ASSAE-GWO-SVM 分类算法准确识别数据敏感度，确保高度敏感信息得到严格保护，而对较低敏感度数据则适度放宽。这种机制有效提升了模型对恶意行为的识别和响应速度，使得即使在恶意行为冲击下，系统也能迅速封锁并控制影响范围，从而保证了整体运行的稳定性。

4 结论

研究提出的 BSSA-NNPP 区块链隐私保护模型通过引入 ASSAE 与 GWO，有效提升了对数据敏感度的分类能力和加密策略的制定。实验结果表明，模型在分类任务中表现出色，准确率最高达到了 95.01%，F_1 分数为 94.23%，召回率和精确率分别为 93.45% 和 95.66%。

这些结果表明，BSSA-NNPP 方案能够准确识别高度敏感信息，并为其实施严格的保护措施，而对较低敏感度数据则采取适度放宽的策略。此外，混淆矩阵分析显示，模型在高度敏感信息分类上表现突出，正确分类 943 个样本；对于较敏感信息，正确分类 981 个，但有 51 个被误判为中等敏感度信息。中等敏感度信息的分类中，931 个样本被正确分类，但与低敏感度信息和较敏感度信息的混淆仍需改进。低敏感度信息的分类效果稍逊，正确分类 981 个。

综上所述，BSSA-NNPP 方案在区块链隐私保护中展现出了良好的性能，尤其是在高度敏感信息的保护方面。然而，模型在低敏感度信息和临时数据的分类上仍存在一定的改进空间。但模型在低敏感度信息和临时数据的分类上仍存在误分类现象，需进一步优化以提升整体性能。

参考文献：

[1] 高丽萍 , 程添 , 高丽 . 区块链环境下基于细粒度授权隐私保护的空间众包任务分配模型 [J]. 小型微型计算机系统 , 2022, 43(4): 759-766.

[2] 王传华 , 张权 , 王慧敏 , 等 . 区块链架构下具有隐私保护的车联网信誉模型 [J]. 浙江大学学报（工学版）, 2023, 57(4): 760-772.

[3] 檀钟盛 , 陈春晖 , 刘书信 , 等 . 区块链环境下的零售物流隐私保护模型 [J]. 重庆理工大学学报 ,2024,38(7):181-188.

[4] 周炜 , 王超 , 徐剑 , 等 . 基于区块链的隐私保护去中心化联邦学习模型 [J]. 计算机研究与发展 ,2022,59(11):2423-2436.

[5] 吴勐 , 戚湧 . 零知识证明下可审计追溯区块链隐私保护模型 [J]. 应用科学学报 ,2024,42(4):598-612.

[6]DEVIDAS S, REKHA N R, SUBBA RAO Y V. Identity verifiable ring signature scheme for privacy protection in blockchain[J]. International journal of information technology, 2023, 15: 2559-2568.

[7] 刘炜 , 唐琮轲 , 马杰 , 等 . 基于区块链和动态评估的隐私保护联邦学习模型 [J]. 计算机研究与发展 ,2023,60(11):2583-2593.

[8] 杨斯博 , 褚晓璇 , 李敏强 , 等 . 区块链技术驱动下数字化平台隐私保护行为演化博弈策略研究 [J]. 工程管理科技前沿 , 2024, 43(4):17-26.

[9] 茆启凡 , 王亮亮 , 王子涵 . 基于隐私保护联邦学习与区块链的图像分类方案 [J]. 计算机应用研究 , 2024,41(2):356-360.

[10]OULD-YAHIA Y, BOUZEFRANE S, BOUCHENEB H, et al. A data-owner centric privacy model with blockchain and adapted attribute-based encryption for internet-of-things and cloud environment[J]. International journal of information and computer security, 2022, 17(3/4):261-284.

[11] 王杨鹏 , 牛宪华 , 熊玲 , 等 . 基于联邦学习和区块链的车联网隐私保护数据共享方案 [J]. 计算机应用 , 2024, 44(z1): 107-111.

[12] 林峰斌 , 王灿 , 吴秋新 , 等 . 基于区块链的工业物联网隐私保护协作学习系统 [J]. 计算机应用研究 , 2024, 41(8): 2270-2276.

[13] 赵文韬 , 官礼和 , 何建国 , 等 . 区块链环境中的隐私保护推荐算法研究 [J]. 计算机工程与科学 ,2024,46(6):1032-1040.

[14] XU J L, LIN J, LIANG W, et al. Privacy preserving personalized blockchain reliability prediction via federated learning in IoT environments[J]. Cluster computing,2022,25:2515-2526.

[15] 张德俊 , 饶元 . 农产品区块链多监管差分隐私共享模型设计 [J]. 江苏农业学报 ,2024,40(4):740-752.

【作者简介】

刘伟伟（1996—），男，山西吕梁人，硕士，研究方向：信息技术、计算机方向。

（收稿日期：2025-05-09 修回日期：2025-09-23）