基于 BiLSTM-GAN 的轨迹隐私保护模型

阎红灿[1,2]，赵雨婷[1]，李思佳[3]，辛禹池[1]

（1.华北理工大学 理学院，河北 唐山 063210；2.河北省数据科学与应用重点实验室，河北 唐山 063210；3.中国人民警察大学 网络舆情研究中心，河北 廊坊 065000）

摘　要：基于位置的服务中，移动轨迹数据的指数级增长使得用户隐私泄露风险问题日益突出，亟需有效的隐私保护机制。为了在保障隐私的同时提升轨迹数据的可用性，构建基于 BiLSTM-GAN 的轨迹隐私保护模型 TCI-BiGAN。利用贝叶斯优化方法实现基于层次密度的含噪声应用空间聚类（HDBSCAN）的自适应调参，提高数据处理效率，降低轨迹冗余度；将 BiLSTM 嵌入生成对抗网络的生成器和鉴别器，利用其上下文特征提取能力高效提取轨迹数据的时空特征，捕捉其依赖关系，使 GAN 生成轨迹与真实轨迹更为相似；通过多元离散型隐马尔可夫模型进行轨迹插值，提高数据的完整性和可用性。在 Foursquare NYC 和 T-Drive 两个真实数据集上，用户轨迹关联准确率分别降低至 0.243、0.198，生成轨迹与真实轨迹的平均豪斯多夫距离分别降低至 0.013、0.019。

关键词：轨迹保护；基于层次密度的含噪声应用空间聚类；双向长短期记忆网络；生成对抗网络；隐马尔可夫模型；轨迹相似度

中图分类号：TP309.2；U495　　**文献标志码**：A　　**doi**：10.13705/j.issn.1671-6833.2026.04.015

基于位置的服务广泛应用于智能出行、社交推荐等领域，产生了海量的轨迹数据[1]。轨迹数据具有极高的应用价值，但也蕴含个人敏感信息，若未经过适当的保护与处理而直接发布，极易导致隐私泄露等安全风险。如何在充分挖掘轨迹数据价值的同时有效防止隐私泄露，已成为研究热点[2]。

轨迹压缩技术旨在保持轨迹特征的前提下，减少数据体量。Ashbrook 等[3]采用了 k-means 算法对轨迹点进行聚类，该方法需要用户预先指定聚类簇的数量，聚类结果不稳定。Ester 等[4]提出基于密度的含噪声空间聚类算法（density-based spatial clustering of applications with noise，DBSCAN），在数据中识别任意形状的簇，被广泛应用于轨迹聚类与压缩，但固定的参数设置难以适应多密度结构。Campello 等[5]提出了基于层次密度的含噪声应用空间聚类（hierarchical density-based spatial clustering of applications with noise，HDBSCAN）算法，在 DBSCAN 的基础上引入层次密度概念，将数据从高密度到低密度逐层聚类，自动确定最优簇结构与噪声点。Yang 等[6]使用梯度阈值处理噪声，应用 DBSCAN 算法对位置点进行聚类，但是算法的输入参数设置高度依赖于主观判断且对结果敏感。申自浩等[7]提出基于稳定隶属度的自动调优多峰值聚类算法，避免了传统聚类算法对簇数或密度阈值的依赖，但是轨迹相似度计算要求轨迹长度一致，影响了在实际应用中的预测准确性。

传统的轨迹合成方法难以充分刻画轨迹数据中复杂的时空依赖关系以及与真实出行行为相关的语义特征，导致生成的合成轨迹在分布特性和行为模式上与真实轨迹存在明显差异，因而容易被攻击者识别。随着人工智能技术的发展，基于深度学习的轨迹合成方法逐渐兴起[8]。一方面，此类方法能够有效弥补传统轨迹合成在时空相关性建模方面的不足，通过学习大规模轨迹数据中的潜在规律，生成更符合真实人类移动模式的合成轨迹，从而更好地反映群体行为特征与移动偏好；另一方面，该类方法在一定程度上降低了用户个人身份遭受重新识别攻击的风险。Kim 等[8]提出一种结合差分隐私机制与深度学习模型的轨迹生成框架，实现对真实轨迹特征

收稿日期：2026-03-05；**修订日期**：206-03-27

基金项目：河北省自然科学基金资助项目（G2024507002）

作者简介：阎红灿（1968—），女，河北保定人，华北理工大学教授，博士，主要从事网络安全、大数据分析与安全研究，E-mail：yanhongcan@ncst.edu.cn。

的模拟。Pan 等[10]基于长短期记忆网络设计虚拟轨迹生成方案,训练分类器区分真实与虚拟轨迹,提升合成轨迹的防攻击能力。Liu 等[11]最早提出利用生成对抗网络生成移动轨迹数据的构想,为轨迹隐私保护提供了新的思路;Rao 等[12]将长短期记忆网络与生成对抗网络融合,提出可生成与真实数据分布相似的轨迹生成模型,但难以捕捉复杂轨迹的长距离依赖关系。Choi 等[13]提出基于生成式对抗模仿学习的轨迹生成框架,将轨迹生成视为部分可观察马尔可夫决策过程中的模仿学习任务,但未充分考虑时间与语义特征。Wang 等[14]设计了基于循环神经网络(recurrent neural network,RNN)与 GAN 的两阶段生成模型,同时引入道路网络信息以增强轨迹合理性。Yang 等[15]基于条件生成对抗网络提出假轨迹生成方法,通过卷积神经网络(convolutional neural network,CNN)提取地图特征,并利用自动编码器推断真实轨迹的运动模式。Shin 等[16]提出了一种基于辅助分类器的生成对抗网络的轨迹生成方法,该方法在提升轨迹多样性与抗识别能力方面具有优势,但轨迹的时序与空间连续性刻画不足。随后,研究者提出融合注意力机制的 GAN 模型[17],注意力机制增强了特征表达能力,但是训练开销较大。

轨迹压缩与轨迹生成阶段之后,轨迹点空间连续性较低。利用轨迹插值模块恢复轨迹时空连续性。早期插值方法多采用几何[18]或统计策略。虽然计算简便,但难以应对非线性变化的真实场景。隐马尔可夫(hidden Markov model,HMM)通过隐状态与观测状态之间的转移与发射概率描述轨迹的演化过程[19],能够在轨迹存在缺失时基于状态推断恢复连续位置点。

本文提出一种基于 BiLSTM-GAN 的轨迹隐私保护模型 TCI-BiGAN(trajectory compression and interpolation for privacy protection based on BiLSTM-GAN),主要贡献如下。

(1)提出一种基于贝叶斯优化的 BO-HDBSCAN(Bayesian optimization-hierarchical density-based spatial clustering of applications with noise)轨迹压缩算法。利用贝叶斯优化实现聚类参数的自适应搜索,降低轨迹冗余度,提高处理效率。

(2)构建一种改进的轨迹生成网络 BiLSTM-GAN。引入能够捕捉双向信息的双向长短期记忆网络,将其嵌入到生成对抗网络中,输入压缩后的轨迹数据使生成对抗网络在训练过程中同时学习轨迹的时空分布与上下文依赖关系,提升合成轨迹的时空一致性,生成与真实轨迹更为相似的合成轨迹。

(3)设计一种 MD-HMM(multivariate discrete-HMM)轨迹插值算法。恢复轨迹的动态特征,提升轨迹数据完整性与可用性。

1 模型设计

TCI-BiGAN 模型由轨迹压缩、轨迹生成和轨迹插值 3 个阶段组成。在轨迹压缩阶段,采用 BO-HDBSCAN 算法为后续生成阶段提供更精简的输入数据。轨迹生成阶段基于压缩后的轨迹特征构建 BiLSTM-GAN 模型,生成接近真实轨迹的隐私保护数据。由于压缩与轨迹生成过程会导致轨迹点分布稀疏,轨迹插值阶段采用 MD-HMM 算法对生成轨迹进行时空补全,提高轨迹数据的完整性与可用性。3 个阶段依次衔接,形成了兼顾隐私保护与数据可用性的完整流程。TCI-BiGAN 模型架构如图 1 所示。

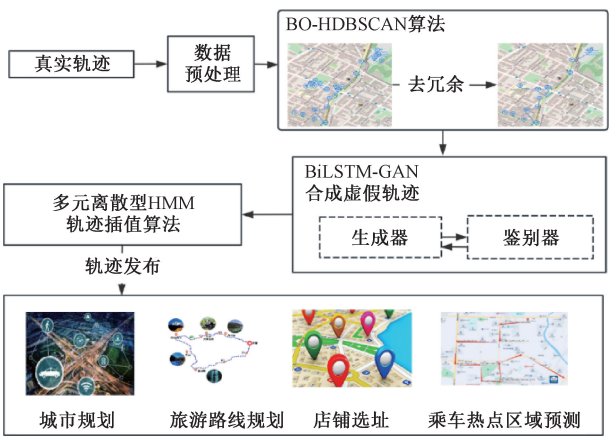


图 1 TCI-BiGAN 模型架构图

Figure 1 Architecture of the TCI-BiGAN model

1.1 设计轨迹压缩算法 BO-HDBSCAN

在 HDBSCAN 算法中,参数 *min_samples* 与 *min_cluster_size* 直接影响簇的识别、噪声的处理及算法的灵活性。由于不同用户轨迹在时空分布上存在差异,每条轨迹都需要不同的超参数,手动设置费时费力。本文提出一种 BO-HDBSCAN 轨迹压缩算法,引入贝叶斯优化方法对 HDBSCAN 参数进行自适应调节。与传统轨迹压缩算法相比,所提方法利用贝叶斯优化实现聚类参数的自适应搜索,避免人工调参;在单条轨迹层面进行聚类与关键点提取,提高了算法对异质轨迹数据的适应性;综合保留起止点、聚类质心与噪声点,兼顾轨迹信息完整性与冗余去除效果。

算法 1 BO-HDBSCAN 轨迹压缩算法

输入:原始轨迹数据集 *TS*;

输出:去冗余后的轨迹数据集 *CleanTS*。

① 初始化压缩后轨迹集合 $CleanTS \leftarrow \varnothing$

② For T in TS do

③ 在参数空间中,利用贝叶斯优化器(TPE 算

法)构建目标函数的概率模型

④ 聚类结果的平均轮廓系数负值为优化目标,通过采集函数迭代更新,搜索获得最优参数组合($min\_samples$,$min\_cluster\_size$);

⑤ HDBSCAN($min\_samples$,$min\_cluster\_size$)对轨迹 T 进行聚类;

⑥ 提取轨迹的起点与终点;

⑦ 对每个聚类簇计算质心坐标,并将其作为代表性关键点;

⑧ 保留噪声点,以增强轨迹特征表达;

⑨ 将所有关键点按时间索引顺序排序,生成压缩后的轨迹 T^*;

⑩ 将 T^* 加入 $CleanTS$;

⑪End For

⑫return $CleanTS$

1.2 构建轨迹生成模型 BiLSTM-GAN

轨迹生成模型如图 2 所示。轨迹数据具有明显的时序性和空间连续性特征,模型采用了基于双向长短期记忆网络的生成结构,使其能够同时捕捉轨迹的前向与后向动态特征,从而更准确地描述个体出行活动的整体规律。联合生成对抗机制,使生成器与鉴别器在博弈过程中不断优化,增强合成轨迹的随机性;并通过多维相似性约束,使其在保持隐私性的同时,保留真实轨迹的整体结构特征。

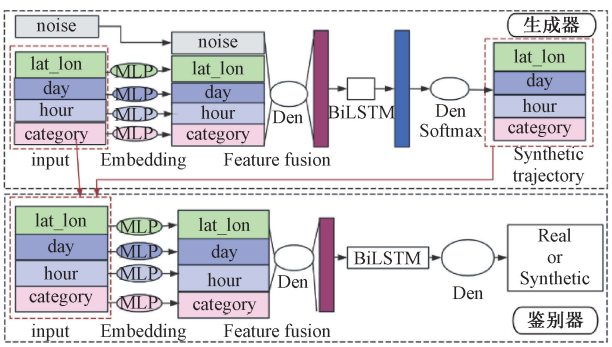


图 2 BiLSTM-GAN 模型结构图

Figure 2 BiLSTM-GAN model architecture

1.2.1 生成器网络架构

生成器生成具有高度真实性和多样性的轨迹数据。生成器网络结构如图 3 所示。

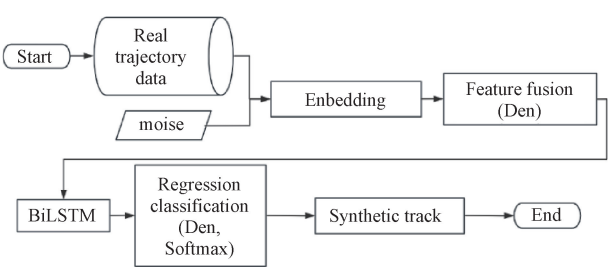


图 3 生成器网络结构图

Figure 3 Generator network architecture

生成器使用多层感知器处理数据集中的位置属性,对于一条长度为 T 的轨迹,记第 i 个轨迹点的原始属性包括相对于轨迹质心的纬度与经度偏移 Δlat_i 和 Δlon_i,日期 one-hot 向量 $\boldsymbol{v}_{\mathrm{d}}^{i} \in \mathbf{R}^{7}$,时间 one-hot 向量 $\boldsymbol{v}_{\mathrm{h}}^{i} \in \mathbf{R}^{24}$,以及类别 one-hot 向量 $\boldsymbol{v}_{\mathrm{c}}^{i} \in \mathbf{R}^{10}$。首先通过多层感知器对各属性进行嵌入:位置偏移嵌入为 $\boldsymbol{a}_{\mathrm{l}}^{i} \in \mathbf{R}^{64}$,日期、时间与类别属性分别嵌入为 $\boldsymbol{a}_{\mathrm{d}}^{i} \in \mathbf{R}^{7}$,$\boldsymbol{a}_{\mathrm{h}}^{i} \in \mathbf{R}^{24}$,$\boldsymbol{a}_{\mathrm{c}}^{i} \in \mathbf{R}^{10}$;$\boldsymbol{W}_{\mathrm{el}}$、$\boldsymbol{W}_{\mathrm{ed}}$、$\boldsymbol{W}_{\mathrm{eh}}$、$\boldsymbol{W}_{\mathrm{ec}}$ 均为可学习权重,激活函数均为 ReLU。计算公式[12]如下所示:

$$\boldsymbol{a}_{\mathrm{l}}^{i} = R_{\mathrm{l}}(\Delta lat_i, \Delta lon_i; \boldsymbol{W}_{\mathrm{el}}); \tag{1}$$

$$\boldsymbol{a}_{\mathrm{d}}^{i} = R_{\mathrm{d}}(\boldsymbol{v}_{\mathrm{d}}^{i}; \boldsymbol{W}_{\mathrm{ed}}); \tag{2}$$

$$\boldsymbol{a}_{\mathrm{h}}^{i} = R_{\mathrm{h}}(\boldsymbol{v}_{\mathrm{h}}^{i}; \boldsymbol{W}_{\mathrm{eh}}); \tag{3}$$

$$\boldsymbol{a}_{\mathrm{c}}^{i} = R_{\mathrm{c}}(\boldsymbol{v}_{\mathrm{c}}^{i}; \boldsymbol{W}_{\mathrm{ec}})。 \tag{4}$$

每个时间步引入随机噪声向量 $\boldsymbol{z}^{i} \in \mathbf{R}^{100}$,将所有嵌入向量与噪声拼接形成融合特征 $\boldsymbol{k}_i^{(\mathrm{row})} = [\boldsymbol{a}_{\mathrm{l}}^{i}; \boldsymbol{a}_{\mathrm{d}}^{i}; \boldsymbol{a}_{\mathrm{h}}^{i}; \boldsymbol{a}_{\mathrm{c}}^{i}; \boldsymbol{z}^{i}] \in \mathbf{R}^{205}$。为获得统一的轨迹点表示,将 $\boldsymbol{k}_i^{(\mathrm{row})}$ 输入至一层包含 100 个单元的全连接层进行非线性映射,将原始拼接特征统一投影为 100 维表示,从而得到固定长度的融合特征 $\boldsymbol{k}_i \in \mathbf{R}^{100}$,将所有时间步的融合特征按时间顺序堆叠,可得轨迹的融合特征矩阵:$\boldsymbol{K} = [\boldsymbol{k}_1, \boldsymbol{k}_2, \cdots, \boldsymbol{k}_T] \in \mathbf{R}^{100T}$。为进一步捕捉轨迹的动态演化规律,采用双向长短期记忆网络建模[20]:

$$\boldsymbol{M} = \mathrm{BiLSTM}(\boldsymbol{K}; \boldsymbol{W}_{\mathrm{BiLSTM}})。 \tag{5}$$

式中:$\boldsymbol{W}_{\mathrm{BiLSTM}}$ 为 BiLSTM 的可学习参数;$\boldsymbol{M} = [\boldsymbol{m}_1, \boldsymbol{m}_2, \cdots, \boldsymbol{m}_T]^{\mathrm{T}} \in \mathbf{R}^{200T}$,$\boldsymbol{m}_i \in \mathbf{R}^{200}$。将输出矩阵 $\boldsymbol{M}$ 中的时间步表示 $\boldsymbol{m}_i$ 分别利用回归分类模块完成轨迹点的细化。生成器输出高相似度的合成轨迹。

1.2.2 鉴别器网络结构

鉴别器判断输入轨迹的真实性。鉴别器的网络结构如图 4 所示。

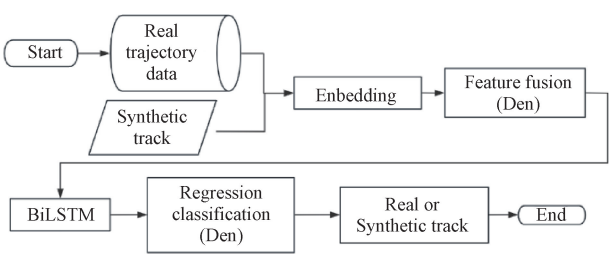


图 4 鉴别器网络结构图

Figure 4 Discriminator network architecture

嵌入层将输入轨迹数据转化为高维向量表示;通过全连接网络对输入特征进行整合;融合后的特征输入至 BiLSTM 层,通过 BiLSTM 层构建轨迹的时间序列特性,以带有时间步的特征作为输入,并产生

一个标量作为输出[20],计算公式如下所示:

$$h = \mathrm{BiLSTM}(\boldsymbol{F};\boldsymbol{W}_{\mathrm{BiLSTM}})。 \quad (6)$$

式中:$\boldsymbol{F}$ 为轨迹中所有轨迹点的融合特征,$\boldsymbol{F} = [\boldsymbol{f}_0;\boldsymbol{f}_1;\cdots;\boldsymbol{f}_{\max\_length}]$;$\boldsymbol{f}_i$ 为第 i 个轨迹点的融合特征向量。回归分类模块输出鉴别结果。

1.2.3 轨迹数据的生成

BiLSTM-GAN 的训练过程是生成器和鉴别器之间的博弈过程,最终达到动态平衡,使生成的轨迹在空间分布和时间特性上接近真实轨迹。设计两个损失函数:L_{D} 用于鉴别器判断轨迹的真伪损失;L_{G} 用于计算生成轨迹的空间、时间和位置点语义损失。L_{D} 函数和 L_{G} 函数[12]分别为

$$L_{\mathrm{D}} = -\frac{1}{N}\sum_{i=1}^{N}(Y_i \cdot \log P(Y_i) + (1 - Y_i) \cdot \log(1 - P(Y_i))); \quad (7)$$

$$L_{\mathrm{G}}(Y_{\mathrm{r}},Y_{\mathrm{p}},\boldsymbol{T}_{\mathrm{r}},\boldsymbol{T}_{\mathrm{s}}) = a \cdot L_{\mathrm{bce}}(Y_{\mathrm{r}},Y_{\mathrm{p}}) + b \cdot L_{\mathrm{s}}(\boldsymbol{T}_{\mathrm{r}},\boldsymbol{T}_{\mathrm{s}}) + c \cdot L_{\mathrm{d}}(\boldsymbol{T}_r,\boldsymbol{T}_s) + d \cdot L_{\mathrm{h}}(\boldsymbol{T}_r,\boldsymbol{T}_s) + e \cdot L_{\mathrm{c}}(\boldsymbol{T}_r,\boldsymbol{T}_s)。 \quad (8)$$

式中:L_{D} 函数使用二元交叉熵,解决二分类问题,评估二分类模型的预测结果;L_{G} 函数中 Y_{r} 和 Y_{p} 分别是真实数据标签和鉴别器的鉴别结果;$\boldsymbol{T}_r$ 和 $\boldsymbol{T}_s$ 分别是真实轨迹和来自生成器的合成轨迹;L_{bce} 为生成器与鉴别器之间的二元交叉熵损失,用于鉴别轨迹相似度,计算公式[21]为

$$L_{\mathrm{bce}}(Y_{\mathrm{r}},Y_{\mathrm{p}}) = -\frac{1}{N}\sum_{i=1}^{N}(Y_{\mathrm{r},i}\log Y_{\mathrm{p},i} + (1 - Y_{\mathrm{r},i})\log(1 - Y_{\mathrm{p},i}))。 \quad (9)$$

记 L_{s} 为空间位置损失,用于约束生成轨迹与真实轨迹在地理坐标上的一致性[22]:

$$L_{\mathrm{s}}(\boldsymbol{T}_r,\boldsymbol{T}_{\mathrm{s}}) = \frac{1}{N}\sum_{i=1}^{N}M_i[(x_i - \hat{x}_i)^2 + (y_i - \hat{y}_i)^2]。 \quad (10)$$

式中:M_i 为轨迹掩码,用于剔除轨迹填充点对损失的干扰;(x_i,y_i) 和 $(\hat{x}_i,\hat{y}_i)$ 分别为真实轨迹点与生成轨迹点的经纬度坐标。

为保证生成轨迹在时间与语义维度上的一致性,本文引入日期损失 L_{d}、时间损失 L_{h} 和类别损失 L_{c},均采用交叉熵形式计算,计算公式[22]分别为

$$L_{\mathrm{d}}(\boldsymbol{T}_{\mathrm{r}},\boldsymbol{T}_{\mathrm{s}}) = -\frac{1}{N}\sum_{i=1}^{N}M_i\sum_{k}y_{\mathrm{r},i,k}^{(\mathrm{d})}\log\hat{y}_{\mathrm{s},i,k}^{(\mathrm{d})}; \quad (11)$$

$$L_{\mathrm{h}}(\boldsymbol{T}_{\mathrm{r}},\boldsymbol{T}_{\mathrm{s}}) = -\frac{1}{N}\sum_{i=1}^{N}M_i\sum_{k}y_{\mathrm{r},i,k}^{(\mathrm{h})}\log\hat{y}_{\mathrm{s},i,k}^{(\mathrm{h})}; \quad (12)$$

$$L_{\mathrm{c}}(\boldsymbol{T}_{\mathrm{r}},\boldsymbol{T}_{\mathrm{s}}) = -\frac{1}{N}\sum_{i=1}^{N}M_i\sum_{k}y_{\mathrm{r},i,k}^{(\mathrm{c})}\log(\hat{y}_{\mathrm{s},i,k}^{(\mathrm{c})})。 \quad (13)$$

式中:$y_{\mathrm{r}}^{(\mathrm{d})}$、$y_{\mathrm{r}}^{(\mathrm{h})}$、$y_{\mathrm{r}}^{(\mathrm{c})}$ 分别为真实轨迹的日期、时间段和位置类别标签;$\hat{y}_{\mathrm{s}}^{(\mathrm{d})}$、$\hat{y}_{\mathrm{s}}^{(\mathrm{h})}$、$\hat{y}_{\mathrm{s}}^{(\mathrm{c})}$ 分别为生成轨迹对应的预测概率分布;i 为轨迹点索引;k 为离散特征类别编号,对日期、时间及位置类别等离散属性在类别维度上求和计算交叉熵损失。

1.3 轨迹的插值重建

设计多元离散型 HMM 轨迹插值算法 MD-HMM,引入隐马尔可夫模型对用户的移动轨迹及其状态转移规律进行多用户建模。通过模型输出的状态概率分布向量,获得用户在某一时间点处于各潜在位置状态的概率。选取高概率的状态进行轨迹合成,实现高效插补。

对历史轨迹数据进行网格化离散,降低轨迹空间表示的复杂度。在模型训练阶段,基于历史轨迹估计状态转移概率和观测发射概率;在轨迹插值阶段,对于轨迹点分布稀疏的片段,输入已编码的观测序列,通过 Viterbi 算法[23]推理出最可能的隐状态路径,还原轨迹的潜在转移过程。

MD-HMM 中的隐状态数量 K 依据用户历史轨迹中的位置类别种类确定,处于 5~10 的可控范围,远小于网格化后的观测空间规模 G,有效避免状态爆炸。在训练阶段,为每位用户独立构建 HMM,估计其初始概率、状态转移概率与观测发射概率。设用户历史轨迹长度为 S,EM 迭代次数为 I,则训练阶段的时间复杂度为 $O(IK^2S)$。由于模型按用户独立训练,可并行化处理,并在网格化降维作用下保证训练效率。在插值阶段,仅对轨迹中存在大间隔的片段执行 Viterbi 推断,单段复杂度为 $O(K^2L)$,整体约为 $O(MK^2L)$,其中 L 为稀疏片段长度,M 为片段的数量。模型空间复杂度为 $O(K^2 + KG)$。

算法 2 MD-HMM 轨迹插值算法

输入:历史轨迹数据 H,待插值轨迹数据 T;

输出:插值后的轨迹集合 T^*。

① 对历史轨迹数据 H 进行网格化离散,构建空间网格映射表 Map

② For 每位用户 do

③ 提取该用户的历史轨迹序列,生成观测序列与状态序列

④ 基于观测序列与状态序列训练多元离散型隐马尔可夫模型 M_{label},估计状态转移概率与观测发射概率

⑤ End For

⑥ For $\tau \in T$ do

⑦ 初始化插值轨迹 $\tau^* \leftarrow \varnothing$;

⑧ 对轨迹中相邻点对 (P_i,P_{i+1}) 计算地理距离 d

⑨ If $d < \theta$, 则将 P_i 加入 τ^*;

⑩ Else

⑪ 将 P_i 加入 τ^*

⑫ 计算应插值点数 $k = \min(N, \lfloor d/\theta \rfloor)$

⑬ 依据模型 M_{label} 当前状态与时间信息，通过 Viterbi 推断最可能的隐状态路径；

⑭ 根据推断结果在 Map 中选取对应网格质心或中心位置作为插值点坐标，构建插值点并加入 τ^*；

⑮ End If

⑯ 将终点加入 τ^*，并存入插值集合 T^*；

⑰ End For

⑱ return T^*

2 实验设计与评估

2.1 数据集

采用 Foursquare NYC[24] 和 T-Drive 数据集[25] 评估算法性能。Foursquare NYC 数据集包含纽约市 193 位用户、3 079 条轨迹共 66 962 个轨迹点。T-Drive 数据集包含北京的 10 357 辆出租车的轨迹，位置总数约为 1 500 万，轨迹总距离约为 9×10^6 km。

2.2 评估指标

轨迹用户连接实验（trajectory user linking，TUL）能够验证模型的隐私保护性能。使用 TUL 算法中多方面轨迹分类器[26] 评估隐私保护策略的有效性：*ACC*@1 表示 Top-1 准确率，即模型预测结果中概率最高的类别与真实标签一致的比例；*ACC*@5 表示 Top-5 准确率，用于衡量模型预测概率排名前 5 的类别中是否包含真实标签；*Macro-F*1 为宏平均精度与宏平均召回率的调和平均值，用于综合反映模型在多类别分类任务中的整体准确性与完整性。

通过比较生成轨迹与真实轨迹在时间分布上的一致性，验证模型在时间上保持数据可用性的能力；通过计算生成轨迹与真实轨迹的豪斯多夫距离（Hausdorff distance，HD）评估模型在空间特征方面保持数据可用性的能力，为一个点集到另一个点集的最远最近点距离[27]：

$$h(A,B) = \max_{a\in A} \min_{b\in B} d(a,b)。 \tag{14}$$

2.3 聚类调参方法对比分析

验证在轨迹压缩过程中引入贝叶斯优化方法对聚类效果的影响，对比 3 种超参数调节方法：贝叶斯优化（Bayesian optimization）[28]、网格搜索（grid search）[29] 和随机搜索（random search）[29]。选取轨迹长度在 70~300 的轨迹并随机采样。贝叶斯优化调参采用 Hyperopt[28] 实现贝叶斯优化策略，设置 $min\_cluster\_size \in [10,15]$，$min\_samples \in [5,10]$；网格搜索穷举搜索参数组合 $min\_cluster\_size \in \{10,12,14\}$、$min\_samples \in \{5,7,9\}$，取聚类轮廓系数最高的一组作为最优参数；随机搜索在参数空间内随机采样，选取最优解。

实验结果如图 5 所示，可以看出使用贝叶斯优化调参轮廓系数更高，效率高于网格搜索；虽然随机搜索用时更短，但是随机搜索的聚类效果较差。贝叶斯优化调参提高了聚类质量和调参效率。

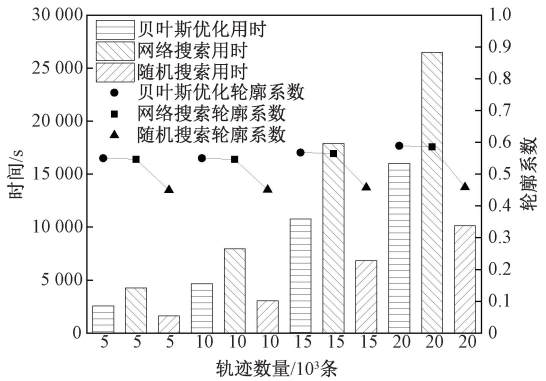


图 5 不同调参方法聚类效果图

Figure 5 Clustering performance with different hyperparameter tuning methods

2.4 隐私保护实验与评估

使用 TUL 检测模型[26] 验证隐私保护能力。表 1 为在 Foursquare NYC 数据集与 T-Drive 数据集中，高斯地理遮蔽（Gaussian geomasking）[30]、TCAC-GAN 模型[16]、AAC-GAN 模型[17] 以及本文 TCI-BiGAN 模型在 TUL 实验中的隐私保护效果。本文模型训练过程中采用 Adam 优化器，学习率设为 0.001，批大小为 256，训练轮次为 2 000 次。

表 1 轨迹用户连接任务中的识别性能对比

Table 1 Comparison of identification performance in trajectory-user linking task

模型	Foursquare NYC			T-Drive		
	ACC@1	*ACC*@5	*Macro-F*1	*ACC*@1	*ACC*@5	*Macro-F*1
Gaussian geomasking	0.486	0.766	0.431	0.421	0.714	0.420
TCAC-GAN	0.309	0.587	0.294	0.289	0.533	0.254
AAC-GAN	0.256	0.515	0.206	0.212	0.511	0.203
TCI-BiGAN	0.243	0.508	0.195	0.198	0.497	0.190

实验结果表明，所提出的 TCI-BiGAN 模型在轨迹用户连接任务中展现出较强的隐私保护能力。因为 T-Drive 数据集来自出租车数据，各用户特征差异明显较小，所以识别准确率略低于 Foursquare NYC 数据集的识别准确率。经过 TCI-BiGAN 处理后的轨迹数据，*ACC*@1、*ACC*@5 与 *Macro-F*1 显著降低，大幅削弱了攻击者对用户身份的推理能力。

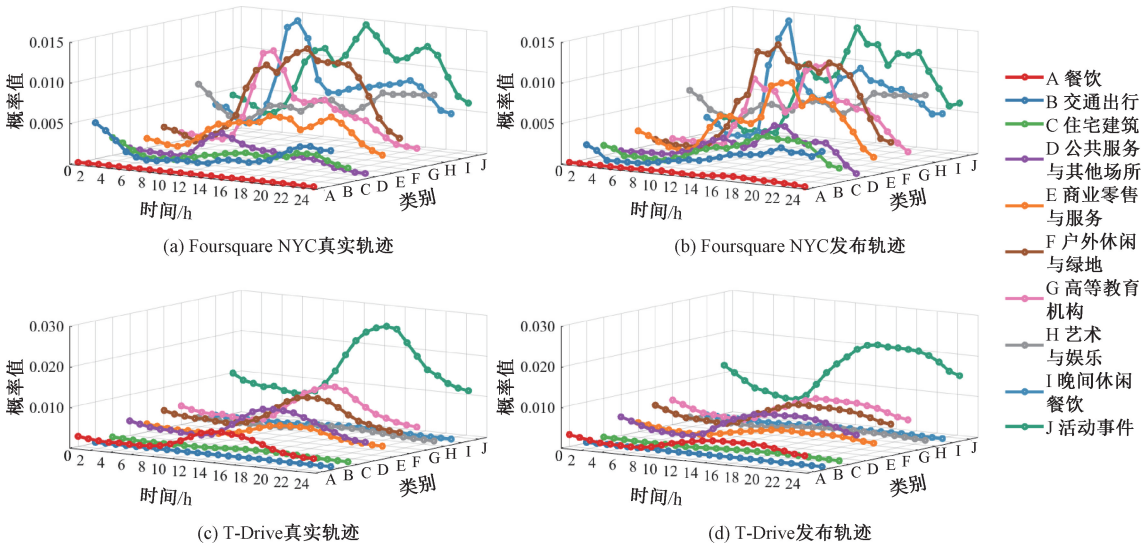
2.5 数据可用实验与评估

2.5.1 时间特征

分析生成轨迹的时间特性保留度。图 6 为真实轨迹和 TCI-BiGAN 模型生成轨迹的位置语义随时间变化的分布情况，展示了餐饮、住宅、娱乐、学校等 10 个类别在 1 d 的访问概率分布趋势。发布轨迹在整体分布趋势、关键语义的活跃时段等方面均与真实轨迹保持高度一致，体现出良好的时间特性保留能力。

2.5.2 空间特征

评估模型的空间特征保留度，实验结果如表 2 所示，可知 TCI-BiGAN 在保持轨迹隐私保护性的同时降低了豪斯多夫距离，提升了轨迹数据的空间一致性与可用性。



(a) Foursquare NYC真实轨迹　(b) Foursquare NYC发布轨迹

(c) T-Drive真实轨迹　(d) T-Drive发布轨迹

图 6　轨迹的位置概率分布图

Figure 6　Spatial probability distribution of trajectories

表 2　利用 Hausdorff Distance 评估空间特征保留度

Table 2　Evaluation of spatial feature preservation using Hausdorff distance

模型	FoursquareNYC				T-Drive			
	Min	*Max*	*Std*	*Mean*	*Min*	*Max*	*Std*	*Mean*
Gaussian geomasking	0.001	0.034	0.005	0.014	0.001	0.042	0.006	0.020
TCAC-GAN	0.004	0.053	0.017	0.016	0.004	0.061	0.018	0.022
AAC-GAN	0.003	0.051	0.016	0.015	0.004	0.060	0.016	0.020
TCI-BiGAN	0.001	0.049	0.015	0.013	0.001	0.056	0.015	0.019

2.5.3 轨迹插值模块性能分析

验证轨迹的插值重建模块对模型性能的影响。在轨迹插值阶段，将经纬度空间划分为分辨率为 0.001°的网格，并以网格编号作为离散观测序列，基于历史轨迹构建离散隐马尔可夫模型，其隐状态数等于轨迹类别数。当相邻轨迹点间的地理距离大于历史轨迹中相邻位置点间距离的平均值时，触发插值过程。实验结果如表 3 所示。

引入插值模块后，虽然 TUL 指标略有上升，但整体变化幅度较小，模型仍能有效削弱攻击者的用户身份推理能力；平均豪斯多夫距离（mean Hausdorff distance，MHD）显著下降。插值模块有效修复轨迹断点、增强时空连续性，使生成轨迹在空间分布上更接近真实轨迹。插值模块在轻微影响隐私保护性能的情况下，显著提升了轨迹的完整性与可用性；在一定程度上实现了隐私与可用性的平衡优化。

表 3　插值前后模型性能对比

Table 3　Performance comparison before and after interpolation

数据集	插值前			插值后		
	ACC@1	*ACC*@5	*MHD*	*ACC*@1	*ACC*@5	*MHD*
Foursquare NYC	0.239	0.480	0.024	0.243	0.508	0.013
T-Drive	0.171	0.378	0.025	0.198	0.497	0.019

3　结论

本文提出了一种基于 BiLSTM-GAN 的轨迹隐私

保护模型 TCI-BiGAN。设计基于贝叶斯优化的 HDBSCAN 自适应轨迹压缩算法,对原始轨迹进行有效简化;将双向长短期记忆网络嵌入生成对抗网络,对轨迹时序特征和分布特性进行建模,生成与真实轨迹在时空分布上高度一致的隐私保护轨迹数据;针对生成轨迹点分布稀疏的问题,设计多元离散型 HMM 轨迹插值算法对轨迹进行时空补全。在 Foursquare NYC 数据集和 T-Drive 数据集上开展评估。TCI-BiGAN 在 TUL 实验中显著削弱了攻击者对用户身份的推理能力,表现出更强的隐私保护效果。同时,合成轨迹在时间分布上与真实轨迹保持高度一致,有效降低了豪斯多夫距离,提高了轨迹的相似性与数据的可用性,在隐私保护与数据可用性之间实现了良好的平衡。

参考文献:

[1] Liu Kai, Wang Jiaqin, Li Hantao. A review of vehicle trajectory prediction based on deep learning[J]. Journal of Zhengzhou University (Engineering Science), 2025, 46(5): 77-89. [刘凯, 汪佳琴, 李汉涛. 基于深度学习的车辆轨迹预测研究综述[J]. 郑州大学学报(工学版), 2025, 46(5): 77-89.]

[2] Li Wenxuan, Wu Hao, Li Changsong. Survey of semantics-based location privacy protection[J]. Journal of Computer Applications, 2023, 43(11): 3472-3483. [李雯萱, 吴昊, 李昌松. 基于语义的位置隐私保护综述[J]. 计算机应用, 2023, 43(11): 3472-3483.]

[3] Ashbrook D, Starner T. Using GPS to learn significant locations and predict movement across multiple users[J]. Personal and Ubiquitous Computing, 2003, 7(5): 275-286.

[4] Ester M, Kriegel H P, Sander J, et al. A density-based algorithm for discovering clusters in large spatial databases with noise[C]//Proceedings of the Second International Conference on Knowledge Discovery and Data Mining. New York: ACM, 1996: 226-231.

[5] Campello R J G B, Moulavi D, Sander J. Density-based clustering based on hierarchical density estimates[C]// Advances in Knowledge Discovery and Data Mining. Cham: Springer, 2013: 160-172.

[6] Yang Peiyu, Zhu Tongyu, Wan Xuejin, et al. Identifying significant places using multi-day call detail records[C]// Proceedings of the 2014 IEEE 26th International Conference on Tools with Artificial Intelligence. Piscataway: IEEE, 2014: 360-366.

[7] Shen Zihao, Tang Yuyu, Wang Hui, et al. Clustering and deep learning based trajectory privacy protection mechanism for Internet of Vehicles[J]. Journal of Zhejiang University (Engineering Science), 2024, 58(1): 20-28. [申自浩, 唐雨雨, 王辉, 等. 基于聚类和深度学习的车联网轨迹隐私保护机制[J]. 浙江大学学报(工学版), 2024, 58(1): 20-28.]

[8] Xu Zhenqiang, Wang Jiayao, Yang Weidong. Research progress in privacy-preserving techniques for trajectory publication[J]. Journal of Geomatics Science and Technology, 2018, 35(1): 87-93. [徐振强, 王家耀, 杨卫东. 面向轨迹数据发布的隐私保护技术研究进展[J]. 测绘科学技术学报, 2018, 35(1): 87-93.]

[9] Kim J W, Jang B. Deep learning-based privacy-preserving framework for synthetic trajectory generation[J]. Journal of Network and Computer Applications, 2022, 206: 103459.

[10] Pan Jiaji, Yang Jingkang, Liu Yining. Dummy trajectory generation scheme based on deep learning[C]//Cyberspace Safety and Security. Cham: Springer, 2019: 511-523.

[11] Liu Xi, Chen Hanzhou, Andris C. trajGANs: using generative adversarial networks for geo-privacy protection of trajectory data (vision paper)[EB/OL]. [2025-12-01]. https://ptal-io.github.io/lopas2018/papers/LoPaS2018_Liu.pdf.

[12] Rao Jinmeng, Gao Song, Kang Yuhao, et al. LSTM-TrajGAN: a deep learning approach to trajectory privacy protection[PP/OL]. V1. arXiv (2020-06-14)[2025-12-01]. https://doi.org/10.48550/arXiv.2006.10521.

[13] Choi S, Kim J, Yeo H. TrajGAIL: generating urban vehicle trajectories using generative adversarial imitation learning[J]. Transportation Research Part C: Emerging Technologies, 2021, 128: 103091.

[14] Wang Xingrui, Liu Xinyu, Lu Ziteng, et al. Large scale GPS trajectory generation using map based on two stage GAN[J]. Journal of Data Science, 2021: 126-141.

[15] Yang Jingkang, Yu Xiaobo, Meng Weizhi, et al. Dummy trajectory generation scheme based on generative adversarial networks[J]. Neural Computing and Applications, 2023, 35(11):8453-8469.

[16] Shin J, Song Yeji, Ahn J, et al. TCAC-GAN: synthetic trajectory generation model using auxiliary classifier generative adversarial networks for improved protection of trajectory data[C]//Proceedings of the 2023 IEEE International Conference on Big Data and Smart Computing (BigComp). Piscataway: IEEE, 2023: 314-315.

[17] Shin J, Song Yeji, Cheong Y Y, et al. Advanced trajectory privacy protection with attention mechanism and auxiliary classifier generative adversarial networks[C]//Proceedings of the 2024 International Conference on Information Networking (ICOIN). Piscataway: IEEE, 2024:

257-261.
[18] Douglas D H, Peucker T K. Algorithms for the reduction of the number of points required to represent a digitized line or its caricature[J]. Cartographica, 1973, 10(2): 112-122.
[19] Ma Shengjie, Wang Pei, Lee H. An enhanced hidden Markov model for map-matching in pedestrian navigation [J]. Electronics, 2024, 13(9): 1685.
[20] Huang Zhiheng, Xu Wei, Yu Kai. Bidirectional LSTM-CRF models for sequence tagging[PP/OL]. V1. arXiv (2015-08-09)[2025-12-01]. https://arxiv.org/abs/1508.01991.
[21] Goodfellow I J, Pouget-Abadie J, Mirza M, et al. Generative adversarial nets[C]//Proceedings of the 28th International Conference on Neural Information Processing Systems. New York: ACM, 2014: 2672-2680.
[22] Goodfellow I, Bengio Y, Courville A. Deep learning [M]. Cambridge, Mass.: MIT Press, 2016.
[23] Bishop C M. Pattern recognition and machine learning [M]. New York: Springer New York, 2006.
[24] Yang Dingqi, Zhang Daqing, Zheng V W, et al. Modeling user activity preference by leveraging user spatial temporal characteristics in LBSNs[J]. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 2015, 45(1): 129-142.
[25] Yuan Jing, Zheng Yu, Xie Xing, et al. Driving with knowledge from the physical world[C]//Proceedings of the 17th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York: ACM, 2011: 316-324.
[26] May Petry L, Leite Da Silva C, Esuli A, et al. MARC: a robust method for multiple-aspect trajectory classification via space, time, and semantic embeddings[J]. International Journal of Geographical Information Science, 2020, 34(7): 1428-1450.
[27] Huttenlocher D P, Klanderman G A, Rucklidge W J. Comparing images using the Hausdorff distance [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 1993, 15(9): 850-863.
[28] Snoek J, Larochelle H, Adams R P. Practical Bayesian optimization of machine learning algorithms [J]. Advances in neural information processing systems. 2012, 4: 2960-2968.
[29] Bergstra J, Bengio Y. Random search for hyper-parameter optimization [J]. Journal of Machine Learning Research, 2012, 13: 281-305.
[30] Gao Song, Rao Jinmeng, Liu Xinyi, et al. Exploring the effectiveness of geomasking techniques for protecting the geoprivacy of Twitter users[J]. Journal of Spatial Information Science, 2019(19): 105-129.

Trajectory Privacy Protection Model Based on BiLSTM-GAN

YAN Hongcan[1,2], ZHAO Yuting[1], LI Sijia[3], XIN Yuchi[1]

(1. College of Science, North China University of Science and Technology, Tangshan 063210, China; 2. Hebei Province Key Laboratory of Data Science and Application, Tangshan 063210, China; 3. Research Center for Network Public Opinion Governance, China People's Police University, Langfang 065000)

Abstract: The exponential growth of mobile trajectory data in location-based services has significantly increased the risk of user privacy leakage, making effective privacy protection mechanisms urgently necessary. To enhance the utility of trajectory data while ensuring privacy protection, a trajectory privacy protection model named TCI-BiGAN was constructed based on BiLSTM-GAN. The Bayesian optimization method was used to perform adaptive parameter tuning for hierarchical density-based spatial clustering of applications with noise(HDBSCAN), improving data processing efficiency and reducing trajectory redundancy. BiLSTM was embedded into both the generator and discriminator of the generative adversarial network to efficiently extract spatiotemporal features and capture dependencies of trajectory data through its contextual feature extraction capability, thereby enhancing the similarity between generated and real trajectories. A multivariate discrete hidden Markov model was applied for trajectory interpolation, increasing data completeness and utility. On the Foursquare NYC and T-Drive real-world datasets, the user trajectory linkage accuracy was reduced to 0.243 and 0.198, respectively, and the average Hausdorff distance between generated and real trajectories was decreased to 0.013 and 0.019, respectively.

Keywords: trajectory protection; hierarchical density-based spatial clustering of applications with noise (HDBSCAN); bidirectional long short-term memory network (BiLSTM); generative adversarial network (GAN); hidden Markov model (HMM); trajectory similarity