软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2023,34(7):3365−3384 [doi: 10.13328/j.cnki.jos.006533]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于跨域关联与隐私保护的深度推荐模型*

王利娥[1,2], 李东城[1,2], 李先贤[1,2]

[1](广西多源信息挖掘与安全重点实验室 (广西师范大学), 广西 桂林 541004)

[2](广西师范大学 计算机科学与工程学院, 广西 桂林 541004)

通信作者: 李东城, E-mail: hatislee@163.com; 李先贤, E-mail: lixx@gxnu.edu.cn

摘　要: 推荐系统能够根据用户的偏好有效地过滤信息, 已被广泛应用于各行各业, 但随着用户数量的爆炸式增长, 数据稀疏性和冷启动问题日益严重. 多源数据融合可以有效缓解数据稀疏和冷启动情况下的推荐精度, 其主要思想是融合用户在其他方面的辅助信息来填补缺失值, 以优化目标服务的推荐准确度, 受到了研究者的青睐, 但由于数据之间的关联引入了更为严重的隐私泄露风险. 针对以上问题, 提出一种基于跨域关联与隐私保护的深度推荐模型, 设计一种具有多源数据融合和差分隐私保护特征的深度学习协同推荐方法. 该方法一方面融合辅助领域信息以提高推荐的精确度, 同时修正异常点的偏差, 改善推荐系统的性能; 另一方面针对数据融合中的数据安全问题, 基于差分隐私模型在协同训练过程中加入噪音以保证数据的安全性. 为了更好地评价推荐系统中的长尾效应, 首次提出一种新的评价指标-发现度, 用以度量推荐算法发现用户隐性需求的能力. 基于已有算法进行了性能对比与分析, 实验结果证明, 所提方法在保证隐私安全的前提下, 比现有方法具有更好的推荐精度和多样性, 能够有效地发现用户的隐性需求.

关键词: 跨域关联; 推荐系统; 差分隐私; 深度学习; 协同训练

中图法分类号: TP309

中文引用格式: 王利娥, 李东城, 李先贤. 基于跨域关联与隐私保护的深度推荐模型. 软件学报, 2023, 34(7): 3365−3384. http://www.jos.org.cn/1000-9825/6533.htm

英文引用格式: Wang LE, Li DC, Li XX. Deep Recommendation Model with Cross-domain Association and Privacy Protection. Ruan Jian Xue Bao/Journal of Software, 2023, 34(7): 3365−3384 (in Chinese). http://www.jos.org.cn/1000-9825/6533.htm

Deep Recommendation Model with Cross-domain Association and Privacy Protection

WANG Li-E[1,2], LI Dong-Cheng[1,2], LI Xian-Xian[1,2]

[1](Guangxi Key Lab of Multi-source Information Mining & Security (Guangxi Normal University), Guilin 541004, China)

[2](School of Computer Science and Engineering, Guangxi Normal University, Guilin 541004, China)

Abstract: Recommendation systems, which can effectively filter information based on user preferences, has been applied widely. The problem of cold start and data sparsity becomes more and more serious with the explosive growth of the number of users. Multi-source data fusion, which can effectively alleviate the recommendation accuracy under the conditions of data sparsity and the cold start problem, is favored by researchers. Its main idea is to fuse auxiliary information of users in other aspects for missing values filling to optimize the accuracy of target recommendation service. Nevertheless, more serious risk of privacy disclosure is introduced due to the relations between data. To solve the above problems, this study proposes a deep cross-domain recommendation model with privacy protection. In detail, a deep learning collaborative recommendation method is designed featuring multi-source data fusion and differential privacy protection. On the one hand, this method fuses auxiliary domain information to improve the accuracy of recommendation and corrects the deviation of abnormal points to improve the performance of the recommender system; on the other hand, this method adds noise in the collaborative

* 基金项目: 国家自然科学基金 (61662008); 广西自然科学基金 (2020GXNSFAA297075); “八桂学者”工程专项, 广西大数据智能与应用人才小高地, 广西区域多源信息集成与智能处理协同创新中心, 广西多源信息挖掘与安全重点实验室系统性研究课题基金 (19-A-02-02)
收稿时间: 2020-11-26; 修改时间: 2021-01-28, 2021-05-17, 2021-10-08; 采用时间: 2021-11-14; jos 在线出版时间: 2022-11-30
CNKI 网络首发时间: 2022-12-01

© 中国科学院软件研究所 http://www.jos.org.cn

training process based on differential privacy model to solve the data security problem in data fusion. In order to evaluate the long tail effect in the recommendation system, this study proposes a new metric—discovery degree for the first time, which is used to measure the ability of the recommendation algorithm to find users' invisible requirements. Based on the performance comparison and analysis of the existing algorithms, the results show that the proposed method has better recommendation accuracy and diversity than the existing methods on the premise of ensuring privacy security, and can effectively discover the hidden needs of users.

Key words: cross-domain association; recommendation system; differential privacy; deep learning; collaborative training

1 引 言

推荐系统是一种信息过滤工具, 它旨在准确地预测用户对商品的偏好程度, 从而把对用户更有价值的商品优先呈现给他们. 随着互联网的迅速发展, 网络上的信息呈指数级增长, 用户面临着严重的信息过载问题. 特别是在电子商务领域, 高质量的推荐系统能够显著的带动用户的活跃性, 有着极其重要的意义. 因此, 如何构建更为精准的推荐系统引起了业界的极大关注, 成为近年来研究者们关注的一个热点问题.

随着数据的日益增长, 推荐系统已不再是一门单一的学科, 而是一门融合了多个学科领域的交叉学科, 包括基于机器学习的数据筛选整合、基于数据挖掘的推荐预测, 基于隐私保护技术的数据安全等. 推荐系统的效果直接影响网站用户的活跃性, 高质量的推荐不仅能够有效地防止用户流失, 还能吸引新的用户加入, 成为有力的工具. 目前推荐系统已被广泛应用于各行各业, 是学术界的研究热点之一, 也是机器学习模型[1]的经典应用. 然而, 随着用户规模和项目数量的急剧增长, 应用最为广泛的协同过滤推荐算法由于数据稀疏和冷启动等问题, 推荐质量大打折扣. 低质量的推荐结果引起的偏差在不同领域会产生不同的结果: 比如在医疗保健领域, 对治疗选择不准确的推荐可能会使患者治疗失败; 而在电子商务中, 糟糕的个性化服务可能会推荐用户不感兴趣的产品或内容, 从而导致用户的流失. 我们发现在现实生活中不同领域的数据之间是存在关联的, 比如某用户在电影领域的数据反映出他喜欢科幻类电影, 那么他必然也会喜欢科幻类的书籍, 也就是在某种程度上来说他们是具有关联性的; 再比如在社交领域, 用户 A 和 B 是亲密朋友, 往往具有相似的兴趣爱好, 如果在电子商务领域, A 是新注册用户, 那么其亲密好友 B 的历史数据可用来分析用户 A 的兴趣偏好, 以缓解用户 A 的冷启动问题. 因此, 我们可以聚合多个相关联领域的数据, 以提高数据稀疏和冷启动情况下的推荐准确度. 也有研究工作[2−4]对领域相关性进行了研究与分析, 给出了不同的分析方法和度量指标, 能够为具体的目标领域选择最合适的辅助领域. 随着研究的开展, 融合多源数据的跨域推荐技术已成为目前学术界和商业界的研究热点.

目前的推荐系统主要面临着以下几个方面的挑战.

(1) 数据的稀疏性和冷启动问题. 传统的推荐系统普遍使用协同过滤作为主要推荐方法, 该方法需要用到用户-项目评分矩阵, 它基于相似用户具有相似偏好的假设进行推荐. 在用户评分信息充足的情况下, 通过相似度的计算, 可以快速为用户找到偏好相似的其他用户, 从而实现协同推荐. 但是, 随着用户和商品数量的急剧上升, 大部分用户只购买了极少数的商品, 使得评分矩阵存在大量的缺失值, 数据极其稀疏, 以致依据稀疏评分矩阵进行相似度计算时会产生较大的偏差, 难以找到真正相似的用户或项目. 此外, 当新用户注册或新商品上架时, 还存在更为极端的冷启动问题, 因为没有任何相关数据, 推荐系统无法基于其历史数据进行相似用户或相似项目的计算, 也就无法产生相应的推荐. 针对该问题, 现有工作主要采用融合具有关联的辅助领域数据来有效缓解数据稀疏的问题, 但随着数据关联的引入, 攻击者也能获得更多的背景知识, 隐私问题更为严重.

(2) 评分与真实情感的差异. 现有的推荐系统主要基于用户对项目的评分来进行推荐分析. 然而, 在现实场景中, 评分却不一定能反映用户的真实爱好, 比如以下两种常见现象: 1) 用户默认好评, 但没有详细的评论. 这种数据往往无法反应用户的真实兴趣, 因为用户本身对项目不一定满意, 却懒得去评论. 因此这种评分数据用于推荐分析会使得最后的推荐结果并不是用户所想要的; 2) 用户评分的同时也进行了评论. 但用户评分和评论情感存在反差, 此时通常评论更具说服力; 但也存在极端情况, 比如恶意差评等现象, 因此需要区分这些与用户情感不符的异常点情况以矫正推荐偏差, 因为异常点的存在会干扰推荐系统的性能[5]. 针对该问题, 现有工作主要基于语义进行评论文本的情感分析, 与评分数据进行融合并修正, 但这类方法只能修正评分与评论存在明显差异的情况, 对于默认好

© 中国科学院软件研究所 http://www.jos.org.cn

评和恶意差评等异常点无法区分.

(3) 长尾效应. 长尾效应是指通常情况下只有少部分需求 (20%) 是共性的, 而绝大部分需求 (80%) 是个性化的, 虽然满足单个需求的物品价值并不高却是大部分的需求, 具有非常客观的前景, 也是目前推荐系统的追求目标. 比如书籍的数量可能有过 100 万种, 传统新华书店上架的都是那些热销书, 大约只有 10 万种; 然而在当当与京东电商平台上, 有超过 50% 的销量却来自这 10 万种热销以外的书籍, 那么这 10 万种以外的书籍就是长尾. 传统的评价指标主要是对推荐的准确率进行评价, 根据用户的显式兴趣偏好进行推荐, 很难发现用户的隐性需求, 但这正是目前推荐算法所追求的目标. 比如你上 B 站搜索一个关键词后, 发现它会推荐很多与这个词相关的东西, 但是却很难发现你目前不知道但心里却很感兴趣的东西. 显然, 隐性需求的发现需要更多维度的数据, 基于知识关联进行特征提取和分析能够建立更为精细的用户画像, 所以这也是目前推荐系统中极具挑战性的难点. 据我们所知, 现有的工作还没有能用于评价用户隐性需求的相关性能指标.

(4) 跨域数据融合造成的隐私问题. 由于推荐系统的本质是通过收集用户的历史数据进行分析, 包括用户个人信息、行为偏好等, 由于数据中包含相当多的敏感信息, 因此存在隐私泄露问题. 此外, 基于数据融合的跨域推荐虽然提升了推荐结果的准确度, 却也进一步增强了攻击者的背景知识, 用户的隐私泄露风险大大增加. 随着人们的信息安全意识逐步增强, 隐私问题已成为制约推荐系统发展的瓶颈问题, 亟待解决. 现有的工作大多关注单域推荐的隐私问题, 然而融合多域数据推荐中的隐私问题由于数据关联的引入更具挑战性.

针对以上问题, 本文提出了一种面向多源数据融合的安全推荐方案, 基于差分隐私模型设计了一种融合跨域关联的深度学习协同推荐方法, 主要贡献归纳如下.

首先, 本文通过融合相关领域数据, 采用数据相关性分析与喜好度预测来提升数据稀疏和冷启动的情况下的推荐精度, 同时设计异常点的去除方法来提高推荐系统的稳定性. 具体来说, 针对评分矩阵数据稀疏和冷启动问题, 设计了一种融合跨域关联数据的深度学习方法, 利用卷积神经网络对相关联的辅助领域数据进行迭代分析预测目标用户的喜好度, 以填补缺失值; 为了提高推荐系统的稳定性, 本文还设计了异常点的去除方法, 对比预测喜好度与用户评分之间的差异, 进行异常点分析和偏差修正, 改善推荐系统的性能.

其次, 针对多域数据融合中的隐私问题, 本文提出一种基于差分隐私的深度推荐方法来解决不同领域数据在融合过程中的隐私问题. 具体来说, 针对数据融合过程中敏感数据存在的隐私风险, 提出在卷积神经网络学习过程中对辅助数据采用多领域融合的关联数据作为输入数据的方式规避隐私问题, 使攻击者无法从卷积神经网络的输出逆推某一辅助领域的原始数据; 而对于目标领域的评分数据, 则采用添加自适应的拉普拉斯噪声的方式, 确保敏感数据的安全性.

最后, 为了更好地评价推荐算法的知识发现能力, 本文首次提出了一种新的评价指标—发现度, 采用在推荐列表中首次出现并被用户选择的项目数与推荐列表长度的比值来计算推荐算法能够发现用户的隐性需求的能力, 用来衡量推荐系统在长尾效应方面的性能, 并基于多个真实数据集与现有相关工作进行了对比分析, 验证了本文模型的性能.

2 相关工作

针对推荐领域中的数据稀疏和冷启动问题, 研究人员发现可以通过对不同领域数据的关联学习来进行有效的缓解, 实现对目标域的推荐, 称为跨域关联, 其本质是融合用户在不同领域中的信息来优化目标服务的推荐准确度. 跨域推荐的主流算法主要可分为传统的跨域关联推荐方法和跨域深度推荐方法两大类.

2.1 跨域关联推荐方法

主流的跨域关联算法主要有以下 2 种: 基于语义关系的跨域推荐[6−9]、基于协同过滤关系的跨域推荐[10−15]. Winoto 等人[6]最早提出跨域推荐的概念, 指出可以基于不同领域的项目属性、标签信息、语义网络关系和关联关系等来建立关联推荐. Fernández-Tobías 等人[7]基于语义网络建立了一个物品跨域推荐的通用框架, 设计了一种方法能够自动提取不同领域之间的关联信息. Yang 等人[8]提出利用标签体系来解决异构问题, 核心思想是基于用户

© 中国科学院软件研究所 http://www.jos.org.cn

博文上的标签和电影标签之间的语义关系为桥梁构建一个多部图, 成功实现了依据微博上的博文来分析用户的偏好, 进而为用户进行电影推荐服务. Li 等人[9]提出基于多领域语义融合的协同过滤推荐方法, 通过语义分析和本体实现跨领域项目相似性计算, 并基于领域相关性对不同领域的数据进行迭代集成, 生成跨领域用户-项目评分矩阵. 但基于语义关系的跨域关联其核心是基于领域知识的聚集规则及实例分类方法, 而不同领域之间的规则和方法差异明显, 从而导致此类推荐实例只适用于特定的应用领域, 不具有普适性.

基于协同过滤的跨域推荐主要是指基于用户或项目的近邻关系、隐语义模型等进行关联推荐. Singh 等人[10]提出一种基于联合矩阵分解 (CMF) 的跨领域推荐算法, 但该模型要求两个矩阵中的用户和项目必须严格一致. Shi 等人[11]基于物品标签在不同领域中往往存在交叉重叠的现象, 设计了一种基于标签的跨域协同过滤方法. Shapira 等人[12]用 Facebook 社交网络中的好友关系来增强目标领域中的用户模型. Jiang 等人[13]提出一种混合的随机漫步方法 (hybrid random walk, HRW), 通过社交网络进行迁移学习, 将不同领域联合起来进行推荐, 但基于用户的协同过滤只能用于用户重合的情况. 因此 Jiang 等人[14]提出一种半监督迁移学习方法来处理跨平台的行为预测. Wang 等人[15]则提出了 TagCDCTR (标签信息跨域协作主题回归) 模型, 通过基于共同标签的跨领域项-项相似性编码, 利用扩展的协作主题建模框架链接相关联的领域, 使所学的项目潜在因子通过领域间关系进行关联, 有助于更全面地捕获项目信息. 但基于协同过滤的跨域推荐算法大都基于一种假设: 不同域之间的用户或物品存在重叠或相互对应关系, 而实际上不同领域间的重叠用户或物品一般数量较少, 因此难以取得较好的推荐效果.

2.2 跨域深度推荐方法

目前深度学习在推荐系统中已得到广泛的应用[16], 其本质是在原有推荐技术的基础上, 融合深度学习技术来强化用户特征训练, 用以缓解推荐系统中的数据稀疏和冷启动等问题, 改善推荐系统的性能和推荐精度. YouTube 在视频推荐中引入了深度神经网络, 使其推荐系统的性能得到进一步提升[17]. 谷歌发布了 wide&deep 推荐系统模型[18], 将传统机器学习算法与深度神经网络相结合, 同时保证了模型的准确性和泛化性. 在传统协同过滤算法的基础上, Lian 等人[19]提出了一种基于深度神经网络 (DNN) 的压缩交互网络模型, 通过该模型可以实现跨域用户的特征学习和特征交互. Shumpei 等人[20]为雅虎新闻提供了一种基于循环神经网络 (RNN) 的新闻推荐系统, 实现了实时推荐. Ying 等人[21]提出了一种基于图卷积神经网络 (GCN) 的推荐模型, 将评分矩阵视为二部图, 在评分图上对顶点进行卷积. 葛尧等人[22]则将用户和商品的异质顶点交互和用户评分的同质顶点交互结合起来, 提出了一种新的基于图卷积网络的推荐算法, 使用两组图卷积操作充分利用两种不同的交互信息, 在一定程度上可以缓解评分数据的稀疏问题. Krishnan 等人[23]则利用密集和稀疏领域共享的领域不变组件来指导神经协同过滤, 以改善在稀疏领域学习的用户和项目表示.

此外, 还有工作提出将评论融入推荐系统会提高推荐的预测精度, McAuley 等人[24]提出了一种融合评论的经典推荐模型 HFT, 将商品评论集与矩阵分解中的隐因子进行融合, 以提高推荐的精确性. 基于 HFT, 李琳等人[25]提出在评论主题与矩阵分解隐因子相结合的基础上, 融合用户和商品评论集作为模型的输入, 以改善模型的学习效果. Zheng 等人[26]首次提出了融合用户和商品评论集的深度学习模型 DeepCoNN, 但该模型存在评论集中有过多冗余信息的问题. 针对该问题, Chen 等人[27]基于该模型提出了 NARRE, 引入注意力机制来去除多余评论的影响, 能够实现评论与评分数据的有效融合, 进而改善模型的评分预测性能. 冯兴杰等人[28]提出了 DeepCLFM, 基于评分矩阵和评论文本提取深层非线性特征向量, 以一、二阶特征项的方式进行融合, 使得用户和商品的隐因子产生交互, 进一步提升推荐性能.

近年来, 有工作将对抗学习和强化学习等技术应用于推荐系统中, 以提高推荐系统的准确度. Li 等人[29]针对跨域推荐中实体链接的特征转移问题, 提出一个基于对抗迁移学习的 ATLRec 模型, 利用对抗学习来生成源域和目标域内用户-项目交互的表示, 以有效地捕获用于跨领域推荐的领域共享特征, 从而更好地链接不同领域的项, 获取跨领域的项-项相关性, 促进领域共享知识的学习. Zhao 等人[30]研究了多 (连续) 场景下的推荐问题, 提出了一种基于强化学习 (RL) 的多智能体推荐方法 (DeepChain), 捕获不同场景之间的序列相关性, 并对多种推荐策略进行联合优化. 基于深度学习的跨域推荐技术凭借其强大的自学习功能和自适应性, 成为目前公认能够有效应对跨

© 中国科学院软件研究所 http://www.jos.org.cn

域推荐的精确性和复杂性的有效手段, 也是当前的研究热点, 但这项技术涉及来源于不同领域的多模态数据, 具有复杂的数据关联, 引入了更为复杂的隐私问题.

2.3 推荐系统中的隐私保护方法

推荐系统中的隐私问题一直受到关注, 早期工作就已经指出推荐系统中存在项目链接攻击, 重识别攻击和 k 近邻 (k-nearest neighbors, KNN) 攻击等隐私问题, 越来越多的研究开始关注推荐系统中的隐私问题, 可归纳为基于隐私保护技术的推荐算法和推荐环境中的其他安全机制两类. 其中基于隐私保护技术的推荐算法主要分为基于 k-匿名的模糊处理和基于差分隐私的加噪扰乱等两类. 其中基于 k-匿名的隐私保护技术[31]主要思想是通过泛化与修改来实现原始数据的隐藏, 使挖掘方无法从数据中提取出原始数据信息或用户与隐私信息的关联, 以达到隐私保护的目的. Hu 等人[32]从添加随机扰动角度提出了一种多层次的隐私保护组合模型, 根据高斯和均匀混合扰动动态划分多个扰动级别, 实现矩阵分解模型的隐私保护. 但是对于用户数据规模大的情况, 基于 k-匿名模型的模糊处理方法使得数据在被泛化后的效用性难以得到保证, 降低了用户体验. 而基于差分隐私的技术[33−35]主要思想是通过添加随机噪音扰乱原有数据, 使得攻击者无法区分或辨别目标节点是否在数据集中, 从而实现隐私保护. 但为了保证数据的效用性, 需要将添加的噪音量控制在一定范围内. Zhang 等人[36]针对加权社交网络的隐私泄露问题, 提出了一种基于差分隐私的隐私保护推荐算法, 基于边权值的变化进行分组, 大大减少了计算量, 支持用户的快速响应和个性化排名. 就已有研究结果来看, 差分隐私应用到推荐系统中在隐私安全性和推荐准确性方面都有很好的保证, 但一旦处于分布式环境或动态环境下时, 根据差分隐私的序列组合性, 随着数据聚合或更新次数的增多会导致每次数据共享时消耗的隐私预算相应减少, 从而使得添加的噪声难以控制, 导致输出结果未能保证较好的推荐准确率.

其他的安全机制主要包括基于分布式体系结构或 P2P 网络, 通过将用户数据存储在本地, 由用户完全操控自己的数据, 以保证用户的数据安全, 或采用安全多方计算技术, 通过密码机制来实现对原始数据的不可见以达到隐私保护的目的. Berkovsky 等人[37]提出了一种只需要部分用户数据就可以获得推荐的 P2P 推荐系统, 以保护用户的隐私安全. 而 Kim 等人[38]在加密向量运算时引入新的数据结构, 提出利用公钥全同态加密和安全多方计算技术实现推荐系统的隐私保护. 然而安全多方计算技术要求推荐服务器实时在线. Tang 等人[39]根据用户社交网络的历史评分数据, 利用公钥全同态加密技术构造了能预测用户对特定物品的评分, 为基于预测评分进行 Top-n 物品推荐提供隐私保护. 然而, 所有相似用户的历史数据都在推荐服务器发布的同一公钥下加密, 无法适用于跨域场景中涉及隶属于不同领域的用户数据场景. Bourse 等人[40]利用公钥全同态加密, 构造了深度离散神经网络中的快速同态计算框架, 尝试实现基于机器学习的安全推荐, 然而该工作未解决密文域上的模型训练问题. 基于以上工作, Wang 等人[41]基于 Paillier 公钥加法同态加密提出具有隐私保护特征的联合多用户词向量的训练模型. 此外, 也有工作提出将多种隐私技术结合起来, 刘国丽等人[42]将安全多方计算理论与随机扰乱技术相结合, 而 Truex 等人[43]将差分隐私技术和多方安全计算结合起来, 提出了一种满足差分隐私保护的联合学习 (federated learning) 方法, 在以高精度生成机器学习模型的同时能有效防止个体隐私泄露. Shaik 等人[44]将全同态加密与机器学习结合起来, 实现具有隐私保护的机器学习. 主要想法是使用机器学习算法对终端用户数据进行预测或分类, 将推荐系统规划为一个多目标多约束优化问题和一个简单的单目标多约束优化问题. Wang 等人[45]则提出了一个具有联合学习和隐私保护功能的跨领域推荐 POI 框架, 采用联合学习框架对用户本地历史数据进行分析, 加密潜在特征分布进行知识迁移, 以保护用户的隐私信息.

但分布式体系结构仍然存在数据传输过程中的隐私风险, 而现有的跨域推荐系统主要利用公钥 (全) 同态加密技术来实现隐私保护, 其主要思想是基于安全多方计算来实现推荐服务器、用户与密码服务提供者 (crypto service provider, CSP) 三者之间的隐私信息不可见, 但是这些方法并未阐述如何在密文的基础上进行辅助数据与目标推荐用户的特征相似性的计算问题. 此外, 基于 CSP 的统一公钥形式不适用跨域推荐场景, 因为其本质上还是单用户多数据模型, 不同领域的数据使用各自域中 CSP 的公钥, 而不是同一个 CSP 的统一公钥进行数据加密, 使得基于密文域上预测模型的建立和推荐结果的计算存在新挑战. 因此, 设计高效的具有隐私保护特征的跨域推

© 中国科学院软件研究所 http://www.jos.org.cn

荐模型是一个具有挑战性的重要问题.

3 预备知识

3.1 差分隐私模型

近年来, 有着严格的数学定义和最强背景知识假设的差分隐私模型近期开始被广泛应用到推荐系统中来, 它专门为交互式查询场景而设计, 十分适用于以数据挖掘、机器学习等为目的的数据统计场景, 其基本思想是对数据集进行添加、删除或修改某一条记录的操作不会对查询结果造成明显的影响, 这样一来攻击者就无法推断攻击目标是否在数据集中.

定义 1. 差分隐私[46]. 若取值为 $Range(A)$ 的随机算法 A 在两个至多只差一条记录的任意数据集 D 和 D'上的结果为 $O(O\in \mathrm{Range}(A))$ 满足不等式:

$$\Pr(A(D)\in O)\leqslant e^{\varepsilon}\times \Pr(A(D')\in O),$$

则称随机算法 A 满足ε-差分隐私. 其中隐私预算ε表示隐私保护的强度, 概率 $\Pr(O)$ 由算法 A 的随机性决定; 可以通过设定参数ε保证算法 A 在任何一条数据记录发生变化时, 算法的输出结果不会发生显著的变化.

差分隐私通过对算法输出结果加入适量噪声来满足安全需求, 其噪声机制主要有 Laplace 机制和指数机制进行保护.

定义 2. Laplace 机制[46]. 对任意一个函数 $f: D\to R^d$, 若随机算法 A 的输出结果 $A(D)$ 满足于等式:

$$A(D)=f(D)+\left(Lap_1\left(\frac{\Delta f}{\varepsilon}\right),Lap_2\left(\frac{\Delta f}{\varepsilon}\right),\ldots,Lap_d\left(\frac{\Delta f}{\varepsilon}\right)\right),$$

则称算法 A 满足ε-差分隐私. 其中 $Lap_i\left(\frac{\Delta f}{\varepsilon}\right)$ 是相互独立的拉普拉斯变量, 噪音量大小与 Δf 成正比, 与ε成反比.

定义 3. 指数机制[47]. 假设数据集 D 经过匿名算法 A 处理后的输出结果为以 $q(D, r)$ 为结果的可用性函数, 其中实体对象 $r\in Range$, $q(D, r)$ 表示实体对象 r 的可用性, Δq 为函数 $q(D, r)$ 的敏感度, 若算法 A 以正比于 $\exp\left(\frac{\varepsilon q(D,r)}{2\Delta q}\right)$的概率从 $Range$ 中选择并输出 r, 那么算法 A 提供ε-差分隐私保护.

拉普拉斯机制主要用于数值数据的加噪, 而指数机制则用于分类数据的扰乱, 使得攻击者无法从查询结果中推断出更多的信息.

3.2 MMF 模型

矩阵分解 (matrix factorization, MF) 的基本原理是从评分矩阵中学习用户与物品在低维隐空间上的表示 (表示为 U 和 V 矩阵), 通过 $U^{\mathrm{T}}V$ 来刻画用户和物品之间的关联性. 比如已有评分矩阵 $R_{n\times m}$, 包括 n 个用户对 m 个项目的评分, 有 $R_{n\times m}=U^{\mathrm{T}}V$, 其中 $U=\{U_1, U_2, \ldots, U_{n-1}, U_n\in R^{n\times k}\}$, 每个 U_i 为 n 维, 表示用户 i 的特征向量; $V=\{V_1, V_2, \ldots, V_{m-1}, V_m\in R^{m\times k}\}$, 每个 V_j 为 m 维, 表示物品 j 的特征向量. 矩阵分解的主要任务是基于已有评分信息来对未打分的项目进行评分预测, 缓解数据稀疏的问题. 我们用 r_{ij} 表示用户 i 对项目 j 的评分, 当 $r_{ij}=0$ 时则认为用户 i 没有对项目 j 评分, k 为低维的隐含特征. 矩阵分解算法通过最小化误差目标函数 $Loss_{mf}$ 来求解两个隐特征矩阵 u_i 和 v_j:

$$Loss_{mf}=\sum_{i=1}^{N}\sum_{j=1}^{M}I_{ij}(r_{ij}-u_i^{\mathrm{T}}v_j)^2+\alpha_u\sum_{i=1}^{n}\|u_i\|^2+\alpha_v\sum_{j=1}^{m}\|v_j\|^2,$$

其中, $u_i\in R^{n\times k}$, $1\leqslant i\leqslant n$, $v_j\in R^{m\times k}$, $1\leqslant j\leqslant m$, 为了防止过拟合引入了参数 $\alpha_u>0$, $\alpha_v>0$.

最小化目标函数的方法主要有最小二乘法和梯度下降法, 这里我们采用小批量梯度下降法, 是批量梯度下降以及随机梯度下降的折中办法, 其主要思想是在每次迭代中选取一定数量的样本对参数进行更新, 以减小收敛所需要的迭代次数, 同时使收敛结果更接近梯度下降的效果.

基于多层感知机的矩阵分解模型 (multilayers matrix factorization, MMF), 其中多层感知机 (multilayer perceptron, MLP) 也叫人工神经网络 (artificial neural network, ANN), 它包括输入层、隐藏层和输出层, 其中隐藏

© 中国科学院软件研究所 http://www.jos.org.cn

层可以有多个, 最简单的 MLP 只含一个隐藏层, 即 3 层的结构, 如图 1 所示. 多层感知机中层与层之间是全连接的 (全连接就是: 上一层的任何一个神经元与下一层的所有神经元都有连接). MLP 的最底层是输入层, 中间是隐藏层, 最后是输出层. 首先它与输入层是全连接的, 假设输入层用向量 X 表示, 则隐藏层的输出就是 $f(W_1X+b)$, W_1 是权重 (也叫连接系数), b 是偏置, 这里的函数 f 取常用的 Softmax 函数. 其实隐藏层到输出层可以看成是一个多类别的逻辑回归, 也就是 Softmax 回归, 所以输出层的结果就是 Softmax(W_1X_1+b).

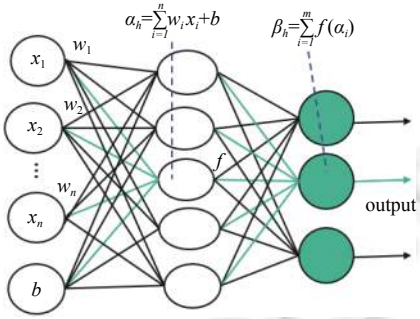


图 1 多层感知机

3.3 One-hot 编码

One-hot 编码主要是采用 N 位状态寄存器来对 N 个状态进行编码, 每个状态都有独立的寄存器位, 并且在任意时候只有一位有效, 它用作分类变量的二进制向量的表示. 这首先要求将分类值映射到整数值. 比如存在以下特征: 性别: [男, 女]; 地区: [武汉, 湖北 (除武汉外), 中国 (除湖北省外)]; 症状: [正常, 干咳, 发热, 呼吸困难]; 按 One-hot 编码原理可将性别特征编码成“男=10”和“女=01” (这里 n=2); 地区特征编码成“武汉=001” “湖北 (除武汉外)=010”和“中国 (除湖北省外)=100” (这里 n=3); 症状特征编码成“正常=0001”“干咳=0010”“发热=0100”和“呼吸困难=1000” (这里 n=4), 因此当一个样本为 [男, 武汉, 呼吸困难] 的时候, 可用数字化的特征 [10, 001, 1000] 来表示.

因此, 我们就可以将离散特征的取值扩展到欧式空间, 使得计算特征之间的距离更加合理, 因为这样一来两个不同分类之间的距离是一样的, 而不会因为编码的原因不合理. 比如不同的职业 1、职业 2 和职业 3, 如果不使用 One-hot, 得到的距离是职业 1 和职业 2 之间的距离是 1, 而职业 1 和职业 3 之间的距离则是 2, 显然这样是不合理的, 因为未必职业 1 和职业 3 之间的距离就更远. 但如果使用 One-hot 编码, 根据欧式距离二维空间的计算公式 $D=\sqrt{(x_1-x_2)^2+(y_1-y_2)^2}$, 则可得到两个职业之间的距离都是 $sqrt(2)$, 即两个职业之间的距离是一样的, 显得更为合理.

4 融合跨域关联和差分隐私保护的深度推荐方法

4.1 系统概述

在本文中, 我们假设推荐系统是可信的, 攻击者可以通过推荐结果, 结合了解的部分用户数据作为背景知识, 去反推目标用户的隐私信息. 本文采用多源数据融合的方法来解决数据稀疏情况下的推荐精度问题并进行异常点的纠偏, 并针对多源数据融合中的隐私安全问题, 基于差分隐私模型设计了一种安全的深度学习跨域协同推荐方法. 本方案包括以下几个方面.

(1) 首先, 为缓解评分矩阵的稀疏性和冷启动问题, 本文采用一种融合不同领域数据作为辅助知识的推荐方法, 利用卷积神经网络对跨域关联数据进行学习, 进而用于预测目标领域中用户对未评分项目的喜好度, 以补全用户-项目评分矩阵中的缺失值, 从而缓解数据稀疏情况下的推荐精度.

(2) 其次, 对于已有评分数据, 本文设计了异常点的分析与去除方法, 提出基于喜好度和评分融合的深度推荐

© 中国科学院软件研究所 http://www.jos.org.cn

模型. 传统的推荐系统往往只考虑用户的评分数据, 而实际上有时候用户的评分并不一定能反映用户对物品的真实兴趣, 甚至是相悖的, 也就是异常点的情况, 而这些异常点的存在往往会影响推荐系统的稳定性. 因此我们考虑利用跨域关联的辅助数据分析得到的用户喜好度来进行异常点的偏差修正, 设计了一种组合函数来捕获预测喜好度与评分的偏差, 偏差超过阈值时即视为异常点, 进行偏差修正或异常点删除, 以过滤无效的干扰数据, 提高推荐系统的性能.

(3) 最后, 本文考虑了多源数据融合中的隐私挑战, 主要从两个方面进行了分析: 一方面是辅助数据的隐私: 为了减少噪声的添加, 这里融合多个领域的关联数据作为卷积神经网络的输入数据, 能够规避隐私泄露风险. 这是因为输入数据并不是个体的原始评分数据, 而是多个邻居在多个领域的数据融合. 另一方面是目标领域评分数据的隐私, 采用差分隐私技术加入随机噪声, 能较好地保证模型的效用性.

4.2 融合跨域关联和差分隐私的深度推荐模型

为了更加清楚的阐述本文方法, 以下结合具体实例来做进一步的详细说明. 整个模型的框架如图 2 所示, 该模型主要分为 3 个模块.

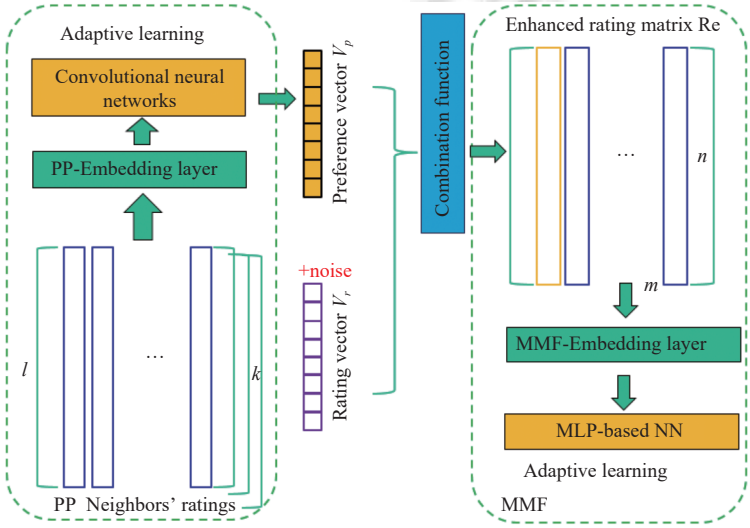


图 2 融合跨域关联和差分隐私的深度推荐模型

(1) 基于跨域关联的喜好度预测模型 (preference prediction, PP). 融合多个辅助领域的关联数据计算出用户对项目的喜好度: 对于缺失值, 可以将用户在辅助领域的数据作为输入, 经过卷积神经网络模型预测出用户对目标领域未评分项目的喜好度, 这样在一定程度上补全了评分矩阵的缺失值, 缓解冷启动情况下的推荐精度.

(2) 异常点去除模块. 设计组合函数整合喜好度和原始评分进行异常点纠偏: 对于已有评分, 当喜好度和用户评分之间存在明显偏差时即视为异常点, 采用组合函数对喜好度和原始评分进行修正处理, 组合函数具体分为 3 种情况, 将后文中进行说明.

(3) 安全推荐模块. 在深度学习过程中, 为了保证用户评分数据的隐私, 对用户原始评分数据注入拉普拉斯随机噪声进行处理. 将基于以上模型得到的具有隐私保护特征的增强版评分矩阵作为 MMF (基于多层感知器的矩阵分解模型)[48]的输入, 学习得到项目的最终预测评分, 并生成推荐列表, 能够有效保护用户的隐私安全.

其具体包括步骤如下.

步骤 1. 预测用户对项目的喜好度. 当前模型的输入为用户在辅助领域的近邻在目标领域的评分数据 V, 其中辅助领域可以为多个不同的领域, 输出为一系列的向量 V_p. 整个学习过程表示为 $V_p = f^{\text{out}}(f^5(\ldots f^2(f^1(V))))$.

步骤 1.1. 第 1 层为 embedding layer, 它将所有用户在辅助领域的数据融合 V 转换为一组特征向量, 从而发现

© 中国科学院软件研究所 http://www.jos.org.cn

用户-项目以及项目-项目之间的关系. 将用户 u 在某一个辅助领域 i 的评分数据表示为一个矩阵 $R_i = R^{(l\times i_p)}$. 对于每个用户的多个辅助领域数据 R_p 在 embedding layer 表示为 $f^1: R_p = \sum_{i=1}^{k} \alpha_i R^{(l\times i_p)}$, 这里 i_p 为需要预测的项目数量, l 表示该领域邻居的数目, k 表示不同领域的数目. 这里的用户 u 在辅助领域的邻居数据表示为 R_p, α_i 是辅助领域的关联系数, 可以根据不同领域的关联度设置不同的优先系数. 然后, 将得到的计算结果 R_p 作为卷积神经网络的输入.

步骤 1.2. 应用 LRP (逐层相关性传播) 算法计算每个输入特征 x_{ij} 对模型输出结果 $F_{x_i}(\theta)$ 之间的相关性, 然后得到每个输入特征的平均相关性 $R_j(D)$, 计算公式如下:

$$R_j(D) = \frac{1}{|D|}\sum_{X_i\in D} R_{x_{ij}}(X_i),$$

其中, D 表示数据集. 在这个步骤中, 由于我们的数据是通过多个领域的相似邻居评分计算得到, 并不是具体的原始评分数据, 不会泄露某个邻居的隐私信息, 因此不需要加噪.

步骤 1.3. 在对神经元进行激活函数处理之前, 对隐含层的神经元进行仿射变换, 公式为 $h_{(x_i)}(W) = b + x_i W^{\mathrm{T}}$, 其中 b 表示神经元的偏置, W 为 h 的参数. 给定一个训练批次 L, h 能写为: $h_L(W) = \sum_{x_i\in L}(b + x_i W^{\mathrm{T}})$.

步骤 1.4. 将卷积层、池化层、全连接层叠加在仿射变换层上构建深度隐私神经网络. 由于访问的数据并不是原始的个体评分数据, 因此计算不会泄露任何信息. 最终的喜好度评分向量表示为 $V_p = f^5(W^5 C_u^m + b^5)$, 这里采用 Softmax 作为输出函数.

步骤 2. 将喜好度和原始评分组合为新的评分.

步骤 2.1. 提取喜好度向量 V_p 中每个用户的预测评分 v_p, 从用户-项目评分矩阵 $R\in R^{n\times m}$ 中提取每一列作为评分向量 v_r.

步骤 2.2. 为了保护用户的隐私, 为评分向量 v_r 添加拉普拉斯噪声 $Lap\left(\frac{\Delta v}{\varepsilon}\right)$ 进行保护, 加噪处理后的评分向量公式为: $\overline{v_r} = v_r + Lap\left(\frac{\Delta v}{\varepsilon}\right)$. 这里 ε 表示隐私预算, 用来控制隐私保护的程度, ε 越小意味着隐私泄露风险越小. 拉普拉斯噪声大小与全局敏感度 $\triangle v$ 密切相关, 这里的 $\triangle v$ 设为 5.

步骤 2.3. 建立一个带有 $\overline{v_r}$ 和 v_p 的联合向量 v_e, 表示为组合函数 $v_e = v_p \otimes \overline{v_r}$. 该函数分为 3 种情况.

1) 如果用户对项目没有进行评分, 则将预测学习得到的喜好度作为评分.

2) 如果用户对一个项目进行了评分, 我们可以通过步骤 1 中计算出喜好度 p_{ui} (即用户 u 对项目 i 的预测喜好度), 从 R 中得到 r_{ui} 的评分. $Bias_{ui} = |p_{ui} - r_{ui}|$ 用来表示预测的喜好度与评分之间的偏差. 如果 $Bias_{ui} \geqslant \rho$, 我们认为当前评分为异常点 (包括恶意差评、习惯好评等情况), 则将忽略 r_{ui}, 直接以 p_{ui} 作为评分. 如果一个用户的评分和喜好度存在差异大于阈值 ρ 的数目超过 l, 则把这个用户当作恶意用户来剔除, 这里的阈值 ρ 和 l 通过学习得出.

3) 如果用户对项目进行了评分, 并且与喜好度的偏差不超过阈值时, 则通过线性加权函数 $v_{ei} = \alpha p_{ui} + (1-\alpha) r_{ui}$ 计算得到评分, 这里我们将 $\alpha \in (0,1)$ 代入函数学习得到.

步骤 3. 由步骤 2 可得到一个增强版的评分矩阵 V_e, 将它作为 MMF 模型的输入, MMF 模型由一个嵌入层和多层感知机组成. 首先, 在嵌入层中使用加权的矩阵分解来实现 user、item 潜在向量的分离. 对于评分矩阵 V_e, users、items 可映射为向量 U_e 和 I_e, 该过程表示为 $V_e = (U_e)^{\mathrm{T}} A I_e$; $U_e \in R^{p\times n}, I_e \in R^{p\times m}$, 这里的 A 是值为 δ 的 $P\times P$ 维对角矩阵. 然后, 使用 one-hot 编码控制神经网络的输入, user 和 item 都通过 one-hot 编码得到稀疏向量, 通过一个 embedding 层映射为用户向量 z_u 和项目向量 z_i, 分别作为控制向量, 最终预测的评分表示如下: $\widetilde{r_{ui}} = h(U_e z_u, I_e z_i | \delta, \gamma)$, 其中 δ 表示嵌入层的参数, γ 表示 MMF 中其他的参数. h 是激活函数, $h^t(U,I) = ReLU(W^t h^{t-1}(U,I) + b^t)$, 其中 $ReLU(x)$=max$(0,x)$, W^t 和 b^t 是第 t 层隐藏层的参数, 可以得到 MMF 的计算公式为: $\widetilde{r} = h^{\mathrm{out}}(h^{T-1}(h^{t-1}(\ldots h^2(h^1(U,I)))))$, $\widetilde{r} = \mathrm{MMF}(V_e|\delta,\gamma)$, 其中 T 是隐藏层的数目, 本文实验中 T 设为 4, MMF 模型如图 3 所示.

图中 MMF 的损失函数如下: $L^{\mathrm{MMF}} = \sum_{u\in U}\sum_{i\in I} W^{\mathrm{MMF}}(r_{ui} - \widetilde{r_{ui}})^2$, W^{MMF} 用来避免过拟合, 然后利用随机梯度下降法来更新参数 δ 与 γ . 至此, 可由评分 $\widetilde{r_{ui}}$ 为用户生成 top-k 推荐列表, 整个推荐过程完成, 具体的算法如算法 1 所示.

© 中国科学院软件研究所 http://www.jos.org.cn

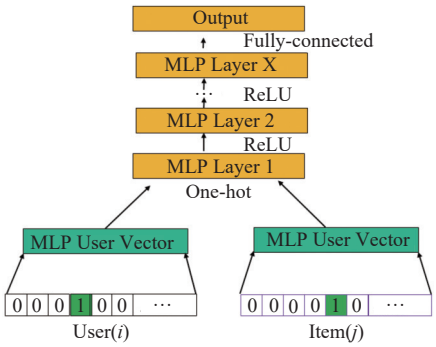


图 3 MMF 模型

算法 1. 融合跨域关联和差分隐私的深度推荐算法.

输入: 训练数据 T_{train}; 隐私预算ε; 组合评分阈值 ρ; 评分向量 v_r;
输出: 推荐列表 *List*.

1. Init P_{matrix}, R_{matrix} //初始化评分矩阵 R_{matrix}, 喜好度矩阵 P_{matrix}
2. **repeat** //训练 CNN 模型
3. $V_p \leftarrow f_{\text{cnn}}(T_{\text{train}})$
4. **until convergence**
5. $P_{\text{matrix}} \leftarrow v_p$
6. $v_r \leftarrow v_r + Lap\left(\frac{\Delta v}{\varepsilon}\right), R_{\text{matrix}} \leftarrow v_r$
7. **Input** P_{matrix}, R_{matrix} to *Combination*(ρ)
8. $V_e \leftarrow$ *Combination*(ρ)
9. **repeat** //训练 MMF 模型
10. $r_u \leftarrow f_{\text{MMF}}(V_e)$
11. **until convergence**
12. top-k *List*$\leftarrow r_u$
13. **return** *List*

5 推荐模型性能分析

5.1 推荐精度

本文所提出的融合跨域关联的深度推荐模型, 对于评分数据的修改主要包括两个部分: 一方面针对数据的稀疏问题, 基于跨域关联的数据采用卷积神经网络进行目标领域的项目喜好度预测分析, 以填补目标领域中评分的缺失值, 缓解数据稀疏带来的推荐不准确问题; 另一方面, 对于异常点进行偏差修正, 这是因为事实上很多用户即使对商品并不满意, 也碍于商家的求好评请求会习惯好评; 或者有些用户懒得进行评分, 系统会生成默认好评; 也存在另一种情况: 虽然用户打的评分不高, 但其实用户对商品本身很满意, 只是对快递的速度或服务不满意, 因此影响了用户的评分. 此外, 还有出于某种自私目的的专业差评和刷好评等现象等也会导致评分不准确. 像以上这些异常点情况, 其实评分数据和用户真实的兴趣爱好是存在偏差的, 如果直接用于预测分析会影响推荐系统的稳定性, 降低推荐性能. 因此, 本文在进行推荐分析时融合辅助领域的跨域数据来进行喜好度分析, 并设计了异常点的去除, 采用组合函数进行权重融合将分析得到的喜好度和原始评分组合为新的评分, 在二者存在明显差异时自动学习并修正偏差, 使得我们的推荐更符合大多数用户的兴趣特征, 从而提高推荐的准确概率. 基于以上分析可知,

© 中国科学院软件研究所 http://www.jos.org.cn

一般情况下, 本文方法会比传统的推荐获得更好的效果.

5.2 安全性

该部分主要从模型训练的两个阶段来进行数据的安全性分析. 第 1 阶段, 本文提出的方法将用户在不同辅助领域的相似邻居对项目的联合评分矩阵作为输入, 经过加权计算得到喜好度, 并不是具体的原始评分数据, 因此攻击者无法通过基于卷积神经网络模型学习得到的喜好度来预测某个领域的原始评分信息, 也就不会泄露某个邻居的隐私信息, 能有效地规避隐私问题. 第 2 阶段, 由于用户的原始评分数据是用户的显式反馈, 如果直接用于分析, 存在一定的隐私泄露风险, 因此本文的方法对用户评分添加了拉普拉斯噪声以保证隐私数据的安全, 然后再分情况进行喜好度和评分数据的融合, 对于异常点进行偏差修正. 下面我们对本文算法的安全性进行严格的理论分析.

定理 1. 算法 1 满足ε-差分隐私.

证明: 具体证明过程如下: 根据差分隐私的定义, 令 $f(\cdot)$ 为函数, D 为数据集, 若随机算法 A 的输出结果 $A(D)$ 满足于等式 $A(D)=f(D)+(Lap_1\left(\frac{\Delta f}{\varepsilon}\right),Lap_2\left(\frac{\Delta f}{\varepsilon}\right),\ldots,Lap_d(\frac{\Delta f}{\varepsilon}))$, 则称算法 A 满足ε-差分隐私.

算法 1 的输入数据分为两个部分: 喜好度矩阵 P_{matrix} 和评分矩阵 R_{matrix}, 其中 $P_{\text{matrix}}\leftarrow V_p$, 而 $V_p\leftarrow f_{\text{cnn}}(T_{\text{train}})$ 是基于多个辅助领域数据的融合, T_{train} 是来源于多个辅助领域的数据; 而 $R_{\text{matrix}}\leftarrow V_r$, V_r 是目标域的评分数据. 由于 V_p 不与个体数据相关联, 而目标领域的用户评分数据 V_r 是与个体相关的敏感数据, 算法 1 中对 V_r 添加了差分隐私噪声, 下面我们将要证明对 V_r 加噪后, 与 V_p 融合后的增强评分矩阵 V_e 也是满足差分隐私的.

对于用户评分 v_r 添加噪声 $Lap\left(\frac{\Delta v}{\varepsilon}\right)$ 后记为 $\overline{v_r}$, 则有 $A(\overline{v_r})=A(v_r)+Lap\left(\frac{\Delta v}{\varepsilon}\right)$, 根据本文的组合函数, 分为 3 种情况, 当无用户评分或者用户评分为异常点时, 直接使用无噪声的预测评分作为用户的评分数据, 自然满足ε-差分隐私; 只有在用户评分和喜好度的预测评分不超过偏差的时候为 $v_{ei}=\alpha p_{ui}+(1-\alpha)\,r_{ui},\ \alpha\in(0,1)$ 则可得到:

$$A(V_e)=f(V_p+\bar{V}_r)=f\left(\sum_{i=1}^{n}\left(\alpha p_{ui}+(1-\alpha)\left(r_{ui}+Lap_i\left(\frac{\Delta r_{ui}}{\varepsilon_i}\right)\right)\right)\right)=f\left(\sum_{i=1}^{n}\left(\alpha p_{ui}+(1-\alpha)r_{ui}+(1-\alpha)Lap_i\left(\frac{\Delta r_{ui}}{\varepsilon_i}\right)\right)\right)$$

$$=f(V_p+V_r)+(1-\alpha)\sum_{i=1}^{n}Lap_i\left(\frac{\Delta r_{ui}}{\varepsilon_i}\right),$$

即可得到组合后的增强评分矩阵 $A(V_e)=A(V_p+\overline{V}_r)\leqslant A(V_p+V_r)+\sum_{i=1}^{n}Lap_i\left(\frac{\Delta f}{\varepsilon_i}\right)$ 即增强评分矩阵 V_e 满足ε-差分隐私定义. 类似的, 我们可以得到 $f_{\text{MMF}}(V_e)=f_{\text{MMF}}(V_p+\overline{V}_r)\leqslant f_{\text{MMF}}(V_p+V_r)+\sum_{i=1}^{n}Lap_i\left(\frac{\Delta f}{\varepsilon_i}\right)$, 即经过 MMF 模型训练得到的推荐结果也就是算法 1 的输出结果满足ε-差分隐私. 因此, 算法 1 满足ε-差分隐私.

5.3 长尾效应

长尾效应显然需要收集更大规模的数据量, 利用多种维度的数据以更加精准地描绘出精细的个性化需求, 才能有效地发现用户的隐性需求, 从而能更好地发挥推荐系统的价值. 传统的推荐系统由于仅依赖用户的评分数据, 而用户的评分数据存在稀疏性和异常点等问题, 影响了推荐系统的性能. 本文提出的方法不仅是基于用户的评分来进行推荐, 同时融合了多个跨域关联的辅助数据, 并基于用户在不同辅助领域的邻居数据进行了缺失值的补充和异常点的修正. 这是根据邻居的兴趣往往存在一定程度相似性的假设, 比如在社交网络中的邻居一般兴趣相投才会成为好友, 而在电影领域的邻居也一定是在该领域的兴趣相似, 那么迁移到目标领域, 其兴趣也一定存在较高的相似度. 因此, 本文融合多领域数据来进行预测分析, 可以从多维度更为全面和精确地去刻画用户的兴趣和爱好, 进而发现用户的隐性需求, 提升推荐系统的性能.

6 实 验

6.1 数据集与评价指标

6.1.1 数据集

数据集采用 Amazon 中来自多个不同领域的真实数据集 https://jmcauley.ucsd.edu/data/amazon, 数据集的具体

© 中国科学院软件研究所 http://www.jos.org.cn

参数如表 1 所示. 本文实验中, 由于数据集的数据量较为庞大, 我们随机取出 10 万条数据进行实验对比, 所有数据集的稀疏度都超过 99.9%. 为了验证跨域关联的推荐效果, 我们选取了具有共同用户集的 Movies and TV, Kindle store, Digital and music 这 3 个相关的数据集, 从中提取跨域关联共同数据集 Cross-domain common data, 其中包括共同 User 数 8 943 个, 涉及的 item 数为 68 485 项, 包括的评分数据 107 601 条, 如表 1 所示. 我们将 Kindle store 与 Movies and TV 数据集作为辅助数据集, Digital and music 数据集作为目标数据集进行了跨域实验. 为了更好地对比验证跨域关联的效果, 同时我们也将目标数据集 Digital and music 按比例 8:2 进行划分, 其中 2 作为辅助领域数据集, 8 作为训练数据, 在训练数据集中再划分 20% 的数据进行测试验证, 给出了实验分析.

表 1　数据集特征

数据集	#User	#item	#rating
Movies and TV	2 088 620	200 941	4 607 047
Kindle store	1 406 890	430 530	3 205 467
Digital music	836 006	478 235	266 414
Cross-domain common data	**8 943**	**68 485**	**107 601**

6.1.2 评价指标

本文主要从 3 个方面来评价推荐系统的性能: 准确率 (accuracy), 多样性 (diversity) 和发现度 (discovery). 其中准确率采用 *RMSE* 和 *F*1-*measure* 两个指标来度量, 多样性针对多次推荐之间的覆盖度来度量, 而发现度是本文针对长尾效应提出的新指标. 正如第 1 节分析的, 长尾效应很关键, 因为如果系统推荐长尾物品给喜欢它们的用户, 其实就是在做“发现”, 向用户展示他喜欢但是不会自己主动发现的物品, 因为他可能并不知道该物品的存在. 最为关键的是, 由于长尾中的物品非常丰富, 如果推荐成功则有可能会为供应商挣得大量的收入和利润, 因此推荐系统的长尾效应非常重要, 基于以上分析, 本文提出一种新的评价指标-发现度作为推荐算法的度量标准.

推荐准确率的常用评价指标均方根误差 (*RMSE*) 表示的是预测值与真实值之间的偏差, 常用于回归模型. *RMSE* 的计算公式为:

$$RMSE=\sqrt{\frac{1}{|\tau|}\sum_{(u,i)\in\tau}\left(\widetilde{r_{ui}}-r_{ui}\right)^2}$$

其中, τ 表示的是测试集, $\widetilde{r_{ui}}$ 表示预测出来的评分, r_{ui} 是测试集的实际评分. 可以看出, *RMSE* 越小意味着预测越准确. 而 *F*1-*measure* 指标综合考虑了准确率和召回率, 是 *Precision* 和 *Recall* 加权调和平均, 是 *IR* (信息检索) 领域的常用的一个评价标准, 常用于评价分类模型的好坏. 这里, 我们采用 *F*1-*measure* 函数来评价推荐方法的效果, 当 *F*1 较高时则能说明该方法比较有效.

$$F1\text{-}measure=\frac{2\times Precision\times Recall}{Precision+Recall}$$

其中, *Precision* (准确率) 是指在推荐给用户的推荐列表中, 用户实际选择的物品数量, 表示为 *Precision*=*c*/*k*, *k* 为推荐列表的长度, *c* 为在推荐列表 *k* 中用户选择的物品数目; *Recall* (召回率) 是指在用户实际评分的物品中被选进推荐列表中的物品数目, 表示为 *Recall*=*c*/*list*(*u*).

Diversity 指标[49]主要用来衡量推荐结果的多样性, 也就是推荐系统能够推荐多种物品的能力, 这里用推荐系统上一次推荐的物品列表与这一次推荐的列表作对比, 两次相差的数据与推荐列表长度的比值来表示: *Diversity* = *diff*/*k*, 其中 $diff=list_1-list_2$ 表示两次相邻推荐的差异数. 为公平起见, 实验结果取多次实验的平均值.

Discovery 指标主要是用来衡量系统挖掘用户潜在兴趣偏好的能力, 发现物品即该物品可能不在用户显式的兴趣范围, 但用户对于它具有较高的潜在满意程度. 这里用推荐列表中首次出现且被用户选择的商品数与推荐列表长度的比值来表示: $Discovery=\frac{|first\cap selected|}{k}$, 其中 *first* 表示在推荐列表中首次出现的物品集合, *selected* 为在推荐列表 *k* 中且被用户选择的物品集合. 这里我们定义的 *first* 为在之前的推荐列表中从未出现过的物品集合,

© 中国科学院软件研究所 http://www.jos.org.cn

也就是新发现的物品, 那么$|first \cap selected|$则是新发现的并且被用户选择的物品数目, 也就是用户的潜在兴趣被发现, 即隐性需求.

6.2 实验对比方法

为了更好地评估本文方法的性能, 我们采用以下几个模型作为本文的对比方法.

1) DPMF[33]: 是集中式的差分隐私推荐方法, 考虑了推荐中的隐私问题, 采用对目标函数添加噪声的方式来满足差分隐私模型, 以保证数据的隐私安全.

2) DP-GD[34]: 是分布式的差分隐私推荐方法, 通过对梯度添加随机噪声来满足差分隐私模型, 该文是本文在推荐精确度方面对比的一个基准线, 由于以上两个方法[27,28]引入的噪声在梯度下降中都会带有信息损失, 通过与它们的对比, 可以检查本文的隐私保护模型在训练过程中能否有效降低信息损失.

3) DeepCoNN[26]: 是首个同时结合用户评论集和商品评论集的深度学习模型, 性能优越.

4) DeepCLFM[28]: 基于 DeepCoNN 模型, DeepCLFM 能够同时利用评分矩阵和评论文本, 而且通过融合多阶特征项的方式完成用户与商品之间的交互, 进一步提升性能. 该文是本文在预测误差方面的对比基线, 由于以上两个方法[26,28]都是考虑了多个数据集的深度学习模型, 但未考虑隐私问题. 通过与它们的对比, 可以检查本文的跨域关联方法能否在保证隐私的同时不影响推荐结果的精确度.

5) TDRS[49]: 是首次提出多样性评价指标的工作, 他指出应该将推荐项目随着时间的推荐发生变化作为推荐评价的一个方面. 该文是本文在多样性评价方面的基线, 通过与它的对比, 可以检查本文的跨域关联能否提高推荐结果的多样性.

6.3 实验结果

本文实验主要从推荐的精度、推荐的多样性和推荐发现度 3 个方面来进行性能的评价与度量, 为了简便, 本文方法缩写为英文简写 DCRM-PP (deep cross-domain recommendation model with privacy protection). 如无特殊说明, 本文提出的 DCRM-PP 方法中的参数设定为 α=0.5, ρ=3, 隐私预算ε的初始设定为 1, 推荐长度 k 默认设为 10, 训练迭代次数为 50.

首先, 本文结合辅助领域的评分, 通过训练组合函数计算的增强评分矩阵得到预测评分. 如表 2 所示, 我们对比了几个方法在不同数据集中的评分误差. 其中 DeepCoNN 和 DeepCLFM 两种方法中并没有考虑隐私问题, 而 DPMF, DP-GD, DCRM-PP 这 3 个方法都结合了差分隐私针对评分进行了隐私保护, 但本文的 DCRM-PP 方法模拟了跨域数据的融合情况, 在数据迭代融合过程中存在一定的信息损失. 尽管如此, 从实验结果来看, DCRM-PP 方法在 *RMSE* 的表现相比 DPMF, DCRM-PP 仍有所降低, 非常接近于没有考虑隐私问题的 DeepCoNN 和 DeepCLFM 方法, 尤其是在跨域关联的共同数据集 (Cross-domain common data) 上的表现明显低于这两种方法, 这是因为本文融合跨域关联数据进行了数据偏差修正, 因此推荐结果优于前两种方法. 这从某种程度上说明了本文方法设计的隐私保护方法对于数据精度的影响非常小, 几乎可以忽略.

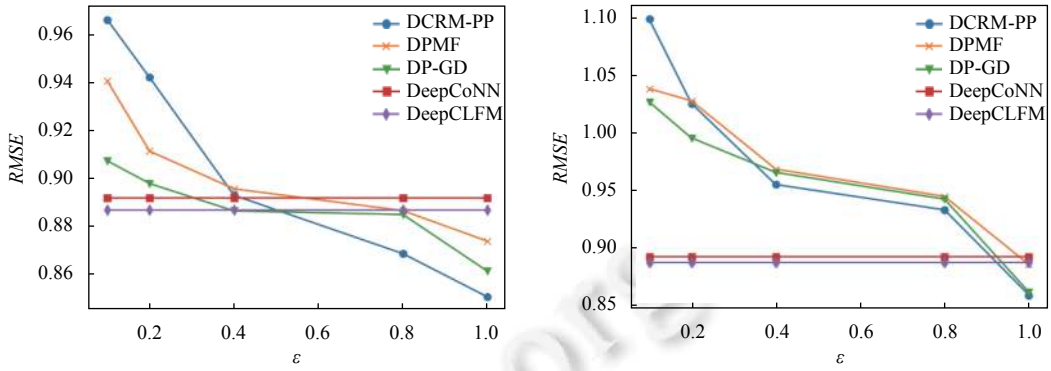
表 2 *RMSE* 对比

数据集	DeepCoNN	DeepCLFM	DPMF	DP-GD	DCRM-PP
Movies and TV	1.009	0.943	1.0814	1.0286	1.0284
Kindle store	0.783	0.775	0.8243	0.7920	0.7846
Digital and music	0.897	0.887	0.874	0.8615	0.8508
Cross-domain common data	0.892	0.883	0.8855	0.865	0.8595

基于隐私问题的考虑, 我们在评分组合时引入差分隐私模型对原始评分注入噪声, 为了更好的观察对于精度预测的影响, 我们变化了隐私预算 ε, 图 4 观察了不同隐私预算 ε 取不同值的时候对推荐精度的影响. 其中图 4(a)和图 4(b) 分别是在数据集 Digital and music 和跨域关联共同数据集 Cross-domain common data 上的表现, 由实验测试观察到在其他两个数据集 Movies and TV 和 Kindle store 上也有相同的趋势, 因此为了节省篇幅, 后面的实验均只在数据集 Digital and music 和跨域关联共同数据集 Cross-domain common data 上进行验证. 在图 4 中,

© 中国科学院软件研究所 http://www.jos.org.cn

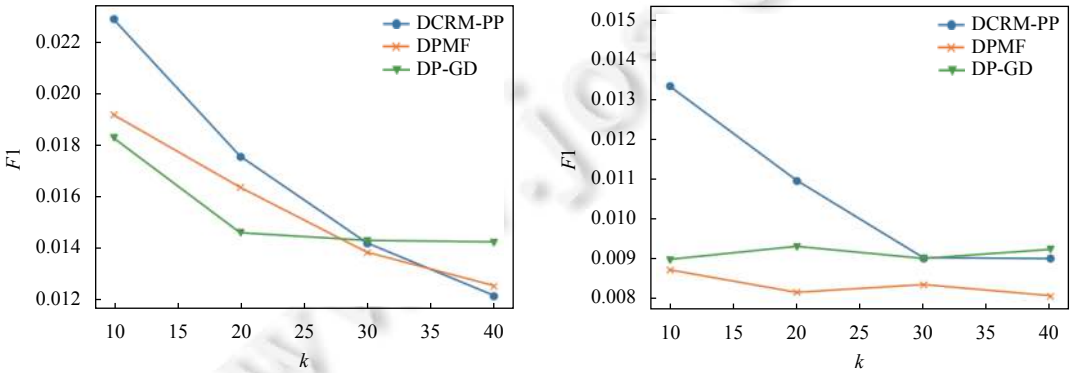
DeepCoNN 和 DeepCLFM 两个方法是没有采用隐私保护方法的, 因此我们直接取模型训练完成后预测评分误差进行对比, 表现为一条横线; 由观察可知, 当 ε 取值较小时, 基于差分隐私模型的方法由于添加的随机噪声过大, 误差相对比较高. 随着隐私预算的不断增大, 训练的错误率也在不断降低. 而本文提出的增强预测模型 DCRM-PP 下降趋势远远快于其他对比方法, 这是因为本文结合了跨域关联评分进行增强评分, 弥补了偏差数据对于训练模型的影响, 大大降低了训练后得到的输入误差, 进而提高了预测精度.



(a) Digital and music (b) Cross-domain common data

图 4 隐私预算ε对于 *RMSE* 的影响

其次, 本文评估了推荐的精确度, 分别从两个不同的数据集中观察不同推荐列表长度 k 和不同隐私预算ε下的推荐精度, 并只基于相关工作 DPMF 和 DP-GD 做了对比, 因为 DeepCoNN, DeepCLFM 没有进行 top-k 的指标度量. 其中图 5 为不同推荐列表长度下的变化结果, 横坐标为推荐列表的长度, 可以看出随着推荐列表长度 k(横坐标) 的增加, *F*1-*measure* 指标结果在不断降低. 相比其他两个方法, 本文方法 DCRM-PP 在推荐列表长度有限的情况下推荐精度相比其他方法优势明显. 但在随着推荐长度的增加, 出现了交叉点, 这是因为推荐长度越长, 用户感兴趣的商品落入列表的概率就会越大, 但在很多情况下需要考虑推荐时效、计算复杂度等问题, 尤其是在资源有限的情况下, 推荐长度过长会导致用户体验满意度下降. 图 6 是在跨域关联共同数据集 Cross-domain common data 上不同隐私预算ε变化对推荐准确度的影响, 其中图 6(a) 为隐私预算ε的变化对于指标 *F*1-*measure* 的影响, 可以看出, 随着隐私预算的增大, 所有方法在 *F*1-*measure* 上的表现都呈现上升趋势, 但本文方法 DCRM-PP 呈现的优势更为明显, 说明本文方法在推荐准确度方面性能更好. 图 6(b) 为隐私预算ε的变化对于指标 *recall* 的影响, 实验结果表明, 所有方法在召回率方面上的表现都呈现较为稳定的趋势, 但本文方法 DCRM-PP 的召回率更高, 说明本文方法能够更准确地将更多用户实际评分的物品选进推荐列表中.

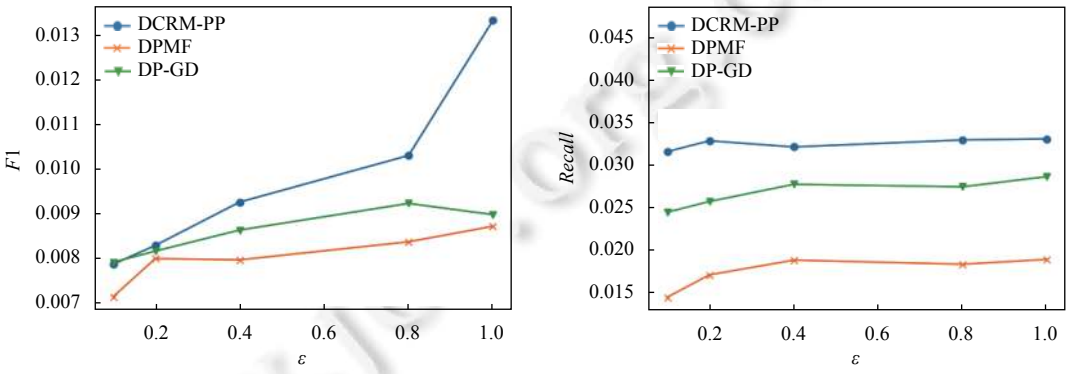


(a) Digital and music (b) Cross-domain common data

图 5 推荐长度对于 *F*1-*measure* 的影响

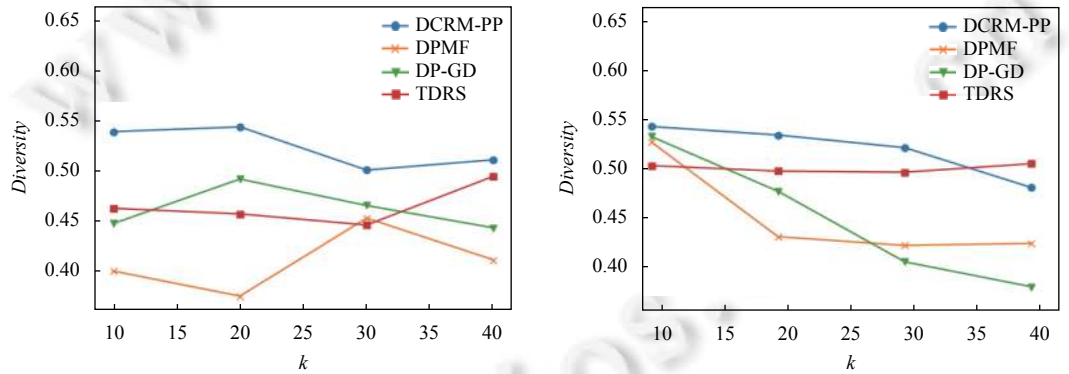
© 中国科学院软件研究所 http://www.jos.org.cn

然后, 我们评估了推荐结果的多样性, 为了更好地进行分析, 我们将首次提出多样性指标的工作 *TDRS* 作为我们的对比基线, 由于 *TDRS* 中的数据集与本文的数据集不一样, 为了公平起见, 在进行对比的时候我们取了两个数据集中的最高点来进行对比, 而本文的多样性结果值取多次试验的平均值. 实验结果如图 7 所示, 从图中结果来看, 随着推荐列表长度的增加, 推荐结果的多样性有所下降, 但这种下降趋势并不明显. 可以看到, 在 Digital and music 数据集上表现并不稳定, 这是因为数据集中项目数目相对稀少, 随着推荐列表长度的增加, 就会更好的囊括用户感兴趣的商品, 而多次推荐之间的差异就会越小. 而在跨域关联的共同数据集上, 数据稀疏性问题得到缓解, 推荐结果的多样性变化趋势相对稳定, 推荐多样性平均在 50% 左右, 明显优于其他方法, 说明本文的方法的跨域关联能够有效改善推荐结果的多样性. 对于在推荐长度为 40 时出现的交叉现象, 原因与上面类似, 这是因为推荐长度越长, 商品的多样性自然就会增加, 但推荐长度过长会导致过多资源的浪费和用户体验满意度下降, 本文方法在推荐长度有限的情况下效果明显更好.



(a) *F*1-*measure* (b) *Recall*

图 6 隐私预算对于推荐准确性的影响



(a) Digital and music (b) Cross-domain common data

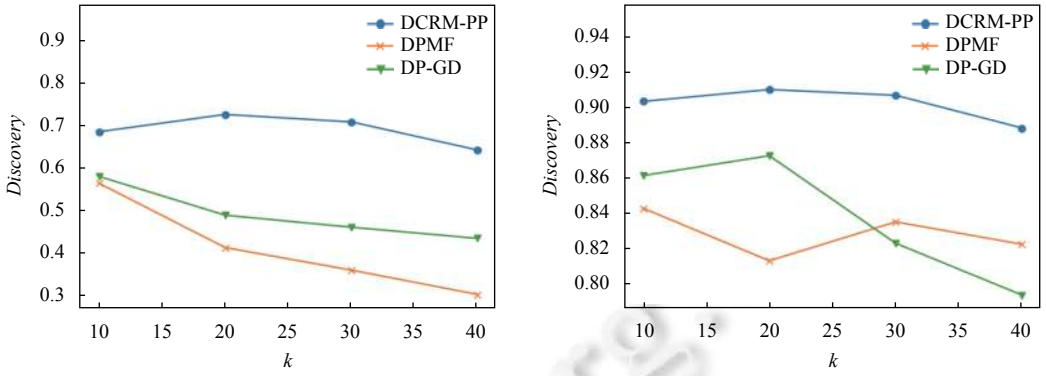
图 7 推荐长度对于 *Diversity* 的影响

接下来, 我们验证了本文新提出的评价指标-发现度, 以推荐列表中首次出现并被用户选中的商品数与推荐列表总数目的比值来度量推荐系统能够发现用户隐性需求的能力. 由于该指标是本文新提出的, 为了对比, 我们重现了考虑隐私问题的 DPMF 和 DP-GD 方法, 并计算其相应的发现度, 实验结果如图 8 所示. 从图中可以看出, 随着推荐长度的变化, 本文的方法 DCRM-PP 始终明显优于其他方法, 且表现稳定. 这是因为本文方法融合了具有跨域关联的辅助评分, 填补了缺失值, 并修正了异常点的评分偏差, 建立了具有更多维特征的、更为精确的用户画像, 提升了推荐算法发现用户隐性需求的能力.

此外, 我们还在跨域关联数据集 Cross-domain common data 上验证了隐私预算ε对于推荐指标 *Diversity* 和

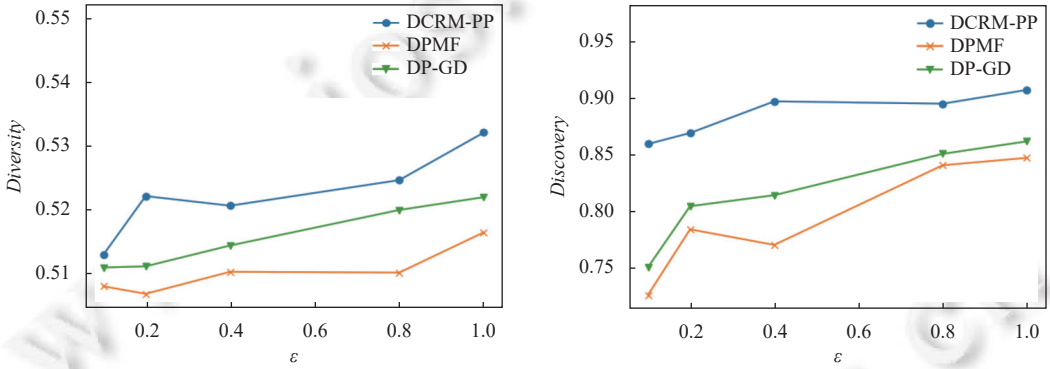
© 中国科学院软件研究所 http://www.jos.org.cn

Discovery 的影响, 结果如图 9 所示. 其中图 9(a) 为推荐多样性 *Diversity* 受隐私预算ε变化的影响, 图 9(b) 为推荐发现度 *Discovery* 受隐私预算ε变化的影响. 可以看出, 随着隐私预算ε的增加, 推荐多样性和发现度均呈现稳定上升趋势, 并没有受到噪音的明显影响.



(a) Digital and music (b) Cross-domain common data

图 8 推荐长度对于 *Discovery* 的影响



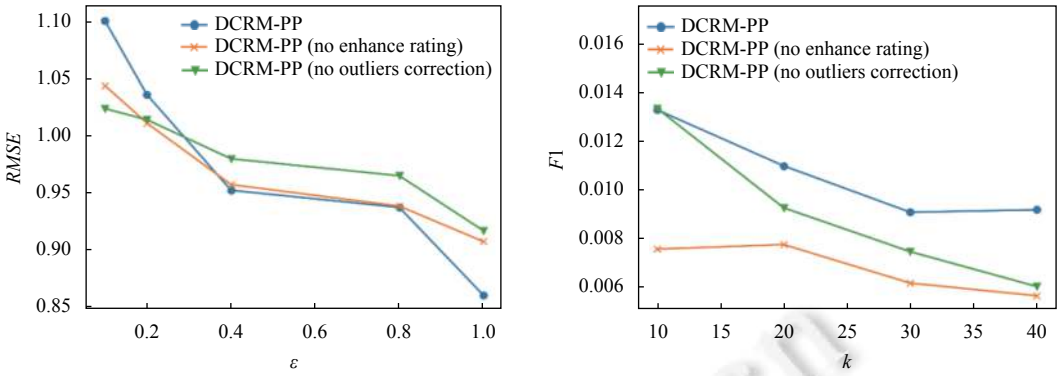
(a) *Diversity* (b) *Discovery*

图 9 隐私预算ε对于 *Diversity* 和 *Discovery* 的影响

最后, 为了检验跨域关联的增强评分与异常点的纠偏效果, 我们在跨域关联数据集 Cross-domain common data 上进行了跨域关联的增强评分和异常点的纠偏对于 *RMSE* 和 *F*1 指标的影响分析, 结果如图 10 所示. 其中图 10(a) 为 *RMSE* 是否受异常点纠偏的影响, 图 10(b) 为 *F*1 是否受异常点纠偏的影响. 其中 DCRM-PP (no enhance rating) 中取消了基于辅助领域进行喜好度预测对评分的增强; DCRM-PP (no outliers correction) 则考虑了基于辅助领域进行喜好度预测对评分的增强, 但没有考虑二者之间的差异, 取消了异常点的纠偏处理. 从图中结果可以看出, DCRM-PP 方法在 *RMSE* 和 *F*1 指标上都要优于没有进行跨域关联增强评分与异常点纠偏的方法效果, 表明本文中异常点的纠偏能够有效地提高推荐精确度.

由以上实验结果可以看出, 基于单个数据集划分与多个数据集关联的共同数据集的实验结果对比, 跨域关联的数据集在各方面的表现都更为稳定, 这就说明本文提出的基于跨域关联的增强预测模型 *DCRM-PP* 能够有效地利用跨域关联知识减少预测评分的误差, 去除异常点的影响, 提升推荐结果的精确度和多样性, 并具有较好的知识发现能力. 此外, *DCRM-PP* 还在模型训练过程中对于原始数据进行了加噪处理, 由第 5.2 节中安全性分析可知, 满足 ε-差分隐私, 能够有效地保证数据安全, 通过图 6、图 9 等的实验结果分析可知, 噪声的加入不影响数据的效用性, 能够保证推荐系统的性能.

© 中国科学院软件研究所 http://www.jos.org.cn



(a) *RMSE* (b) *F*1

图 10 跨域关联的增强评分与异常点的纠偏对于 *RMSE* 和 *F*1 的影响

7 结 论

本文同时关注推荐系统中的数据稀疏和数据安全问题, 提出一种融合跨域关联数据和差分隐私的深度推荐模型. 首先通过融合跨域关联数据来缓解数据稀疏性和冷启动情况下的推荐精度问题, 然后基于差分隐私模型来解决数据融合过程中存在的隐私安全问题, 同时设计了异常点去除方法, 来提高推荐系统的性能. 具体来说, 我们基于卷积神经网络技术融合跨域关联数据来预测用户对目标领域的项目喜好度, 并通过添加拉普拉斯噪声来保护学习过程中用户评分数据的隐私安全; 其次, 利用预测得到的喜好度一方面用来填补没有评分的缺失值, 以缓解数据稀疏问题; 另一方面用来对比与已有评分之间的差异, 进行异常点的分析与偏差修正, 提高推荐的精确性和多样性, 改善推荐系统的稳定性; 最后, 本文还提出一种新的评价指标: 发现度-用于衡量推荐系统能够发现用户隐性需求的能力. 实验结果表明, 相比现有的推荐方法, 本文方法能够在保证隐私安全的前提下, 具有更好的推荐精确度和知识发现能力, 提升了推荐系统的性能.

References:

[1] Jordan MI, Mitchell TM. Machine learning: Trends, perspectives, and prospects. Science, 2015, 349(6245): 255–260. [doi: 10.1126/science.aaa8415]

[2] Berkovsky S, Goldwasser D, Kuflik T, Ricci F. Identifying inter-domain similarities through content-based analysis of hierarchical Web-directories. In: Proc. of the 17th European Conf. on Artificial Intelligence (ECAI 2006). Riva del Garda: IOS Press, 2006. 789–790.

[3] Yi C, Shang MS, Zhang QM. Auxiliary domain selection in cross-domain collaborative filtering. Applied Mathematics & Information Sciences, 2015, 9(3): 1375–1381.

[4] Sahebi S, Brusilovsky P. It takes two to Tango: An exploration of domain pairs for cross-domain collaborative filtering. In: Proc. of the 9th ACM Conf. on Recommender Systems. Vienna: ACM, 2015. 131–138. [doi: 10.1145/2792838.2800188]

[5] Al-Qasem Al-Hadi IA, Sharef NM, Sulaiman N, Mustapha N. Ensemble divide and conquer approach to solve the rating scores' deviation in recommendation system. Journal of Computer Science, 2016, 12(6): 265–275. [doi: 10.3844/jcssp.2016.265.275]

[6] Winoto P, Tang T. If you like the devil wears prada the book, will you also enjoy the devil wears prada the movie? A study of cross-domain recommendations. New Generation Computing, 2008, 26(3): 209–225. [doi: 10.1007/s00354-008-0041-0]

[7] Fernández-Tobías I, Cantador I, Kaminskas M, Ricci F. A generic semantic-based framework for cross-domain recommendation. In: Proc. of the 2nd Int'l Workshop on Information Heterogeneity and Fusion in Recommender Systems. Chicago: ACM, 2011. 25–32. [doi: 10.1145/2039320.2039324]

[8] Yang DQ, He JR, Qin HZ, Xiao YH, Wang W. A graph-based recommendation across heterogeneous domains. In: Proc. of the 24th ACM Int'l on Conf. on Information and Knowledge Management. Melbourne: ACM, 2015. 463–472. [doi: 10.1145/2806416.2806523]

[9] Li X, He JS, Zhu NF, Hou ZQ. Collaborative filtering recommendation based on multi-domain semantic fusion. In: Proc. of the 44th IEEE Annual Computers, Software, and Applications Conf. (COMPSAC). Madrid: IEEE, 2020. 255–261. [doi: 10.1109/COMPSAC48688.2020.00041]

© 中国科学院软件研究所 http://www.jos.org.cn

[10] Singh AP, Gordon GJ. Relational learning via collective matrix factorization. In: Proc. of the 14th ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. Las Vegas: ACM, 2008. 650–658. [doi: 10.1145/1401890.1401969]

[11] Shi Y, Larson M, Hanjalic A. Tags as bridges between domains: Improving recommendation with tag-induced cross-domain collaborative filtering. In: Konstan JA, Conejo R, Marzo JL, Oliver N, eds. User Modeling, Adaption and Personalization (UMAP 2011). Lecture Notes in Computer Science. Girona: Springer, 2011, 6787. 305–316. [doi: 10.1007/978-3-642-22362-4_26]

[12] Shapira B, Rokach L, Freilikhman S. Facebook single and cross domain data for recommendation systems. User Modeling and User-adapted Interaction, 2013, 23(2): 211–247. [doi: 10.1007/s11257-012-9128-x]

[13] Jiang M, Cui P, Chen XM, Wang F, Zhu WW, Yang SQ. Social recommendation with cross-domain transferable knowledge. IEEE Trans. on Knowledge and Data Engineering, 2015, 27(11): 3084–3097. [doi: 10.1109/TKDE.2015.2432811]

[14] Jiang M, Cui P, Yuan NJ, Xie X, Yang SQ. Little is much: Bridging cross-platform behaviors through overlapped crowds. In: Proc. of the 30th AAAI Conf. on Artificial Intelligence. Phoenix: AAAI Press, 2016. 13–19.

[15] Wang JQ, Lv J. Tag-informed collaborative topic modeling for cross domain recommendations. Knowledge-based Systems, 2020, 203: 106119. [doi: 10.1016/j.knosys.2020.106119]

[16] Ouhbi B, Frikh B, Zemmouri E, Abbad A. Deep learning based recommender systems. In: Proc. of the 5th IEEE Int'l Congress on Information Science and Technology (CiSt). Marrakech: IEEE, 2018. 161–166. [doi: 10.1109/CIST.2018.8596492]

[17] Covington P, Adams J, Sargin E. Deep neural networks for YouTube recommendations. In: Proc. of the 10th ACM Conf. on Recommender Systems. Boston: ACM, 2016. 191–198. [doi: 10.1145/2959100.2959190]

[18] Cheng HT, Koc L, Harmsen J, Shaked T, Chandra T, Aradhye H, Anderson G, Corrado G, Chai W, Ispir M, Anil R, Haque Z, Hong LC, Jain V, Liu XB, Shah H. Wide & deep learning for recommender systems. arXiv:1606.07792v1, 2016.

[19] Lian JX, Zhou XH, Zhang FZ, Chen ZX, Xie X, Sun GZ. xDeepFM: Combining explicit and implicit feature interactions for recommender systems. In: Proc. of the 24th ACM SIGKDD Int'l Conf. on Knowledge Discovery & Data Mining. London: ACM, 2018. 1754–1763. [doi: 10.1145/3219819.3220023]

[20] Okura S, Tagami Y, Ono S, Tajima A. Embedding-based news recommendation for millions of users. In: Proc. of the 23rd ACM SIGKDD Int'l Conf. on Knowledge Discovery and Data Mining. Halifax: ACM, 2017. 1933–1942. [doi: 10.1145/3097983.3098108]

[21] Ying R, He RN, Chen KF, Eksombatchai P, Hamilton WL, Leskovec J. Graph convolutional neural networks for Web-scale recommender systems. In: Proc. of the 24th ACM SIGKDD Int'l Conf. on Knowledge Discovery & Data Mining. London: ACM, 2018. 974–983. [doi: 10.1145/3219819.3219890]

[22] 0zGe Y, Chen SC. Graph convolutional network for recommender systems. Ruan Jian Xue Bao/Journal of Software, 2020, 31(4): 1101–1112 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5928.htm [doi: 10.13328/j.cnki.jos.005928]

[23] Krishnan A, Das M, Bendre M, Yang H, Sundaram H. Transfer learning via contextual invariants for one-to-many cross-domain recommendation. In: Proc. of the 43rd Int'l ACM SIGIR Conf. on Research and Development in Information Retrieval. Xi'an: ACM, 2020. 1081–1090. [doi: 10.1145/3397271.3401078]

[24] McAuley J, Leskovec J. Hidden factors and hidden topics: Understanding rating dimensions with review text. In: Proc. of the 7th ACM Conf. on Recommender Systems. Hong Kong: ACM, 2013. 165–172. [doi: 10.1145/2507157.2507163]

[25] Li L, Liu JH, Meng XF, Su C, Li X, Zhong L. Recommendation models by exploiting rating matrix and review text. Chinese Journal of Computers, 2018, 41(7): 1559–1573 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2018.01559]

[26] Zheng L, Noroozi V, Yu PS. Joint deep modeling of users and items using reviews for recommendation. In: Proc. of the 10th ACM Int'l Conf. on Web Search and Data Mining. Cambridge: ACM, 2017. 425–434. [doi: 10.1145/3018661.3018665]

[27] Chen C, Zhang M, Liu YQ, Ma SP. Neural attentional rating regression with review-level explanations. In: Proc. of the 2018 World Wide Web Conf. Lyon: Int'l World Wide Web Conf. Steering Committee, 2018. 1583–1592. [doi: 10.1145/3178876.3186070]

[28] Feng XJ, Zeng YZ. Joint deep modeling of rating matrix and reviews for recommendation. Chinese Journal of Computers, 2020, 43(5): 884–900 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2020.00884]

[29] Li Y, Xu JJ, Zhao PP, Fang JH, Chen W, Zhao L. ATLRec: An attentional adversarial transfer learning network for cross-domain recommendation. Journal of Computer Science and Technology, 2020, 35(4): 794–808. [doi: 10.1007/s11390-020-0314-8]

[30] Zhao XY, Xia L, Zou LX, Liu H, Yin DW, Tang JL. Whole-chain recommendations. In: Proc. of the 29th ACM Int'l Conf. on Information and Knowledge Management. ACM, 2020. 1883–1891. [doi: 10.1145/3340531.3412044]

[31] Casino F, Domingo-Ferrer J, Patsakis C, Puig D, Solanas A. A k-anonymous approach to privacy preserving collaborative filtering. Journal of Computer and System Sciences, 2015, 81(6): 1000–1011. [doi: 10.1016/j.jcss.2014.12.013]

[32] Hu ZY, Luo YL, Zheng XY, Zhao YN. A novel privacy-preserving matrix factorization recommendation system based on random perturbation. Journal of Intelligent & Fuzzy Systems, 2020, 38(4): 4525–4535. [doi: 10.3233/JIFS-191287]

© 中国科学院软件研究所 http://www.jos.org.cn

[33] Hua JY, Xia C, Zhong S. Differentially private matrix factorization. In: Proc. of the 24th Int'l Conf. on Artificial Intelligence (IJCAI 2015). Buenos Aires: AAAI Press, 2015. 1763–1770.

[34] Shin H, Kim S, Shin J, Xiao XK. Privacy enhanced matrix factorization for recommendation with local differential privacy. IEEE Trans. on Knowledge and Data Engineering, 2018, 30(9): 1770–1782. [doi: 10.1109/TKDE.2018.2805356]

[35] He M, Chang MM, Wu XF. A collaborative filtering recommendation method based on differential privacy. Journal of Computer Research and Development, 2017, 54(7): 1439–1451 (in Chinese with English abstract). [doi: 10.7544/issn1000-1239.2017.20160207]

[36] Zhang LJ, Zhu XY, Ma JF, Ma Z, Yuan DN. Medical privacy-preserving service recommendation. In: Proc. of the 2020 IEEE Int'l Conf. on Communications (ICC 2020). Dublin: IEEE, 2020. 1–6. [doi: 10.1109/ICC40277.2020.9148641]

[37] Berkovsky S, Eytani Y, Kuflik T, Ricci F. Hierarchical neighborhood topology for privacy enhanced collaborative filtering. In: Proc. of the 2006 Workshop on Privacy-enhanced Personalization (PEP06, CHI 2006). Montreal, 2006. 6–13.

[38] Kim S, Kim J, Koo D, Kim Y, Yoon H, Shin J. Efficient privacy-preserving matrix factorization via fully homomorphic encryption: Extended abstract. In: Proc. of the 11th ACM on Asia Conf. on Computer and Communications Security. Xi'an: ACM, 2016. 617–628. [doi: 10.1145/2897845.2897875]

[39] Tang Q, Wang J. Privacy-preserving context-aware recommender systems: Analysis and new solutions. In: Pernul G, Ryan PYA, Weippl E, eds. Computer Security (ESORICS 2015). Lecture Notes in Computer Science. Vienna: Springer, 2015. 101–119. [doi: 10.1007/978-3-319-24177-7_6]

[40] Bourse F, Minelli M, Minihold M, Paillier P. Fast homomorphic evaluation of deep discretized neural networks. In: Shacham H, Boldyreva A, eds. Advances in Cryptology (CRYPTO 2018). Lecture Notes in Computer Science. Santa Barbara: Springer, 2018. 483–512. [doi: 10.1007/978-3-319-96878-0_17]

[41] Wang Q, Du MX, Chen XY, Chen YJ, Zhou P, Chen XF, Huang XY. Privacy-preserving collaborative model learning: The case of word vector training. IEEE Trans. on Knowledge and Data Engineering, 2018, 30(12): 2381–2393. [doi: 10.1109/TKDE.2018.2819673]

[42] Liu GL, Li A, Li YP, Yu LM. Privacy-preserving technology research on collaborative filtering recommendation algorithm between systems. Application Research of Computers, 2017, 34(9): 2804–2807 (in Chinese with English abstract). [doi: 10.3969/j.issn.1001-3695.2017.09.053]

[43] Truex S, Baracaldo N, Anwar A, Steinke T, Ludwig H, Zhang R, Zhou Y. A hybrid approach to privacy-preserving federated learning. In: Proc. of the 12th ACM Workshop on Artificial Intelligence and Security. London: ACM, 2019. 1–11. [doi: 10.1145/3338501.3357370]

[44] Shaik I, Singh AK, Narumanchi H, Emmadi N, Bhattachar RMA. A recommender system for efficient implementation of privacy preserving machine learning primitives based on FHE. In: Dolev S, Kolesnikov V, Lodha S, Weiss G, eds. Cyber Security Cryptography and Machine Learning (CSCML 2020). Lecture Notes in Computer Science, vol. 12161. Be'er Sheva: Springer, 2020. 193–218. [doi: 10.1007/978-3-030-49785-9_13]

[45] Wang LE, Wang YH, Bai Y, Liu P, Li XX. POI recommendation with federated learning and privacy preserving in cross domain recommendation. In: Proc. of the 2021 IEEE Conf. on Computer Communications Workshops. Vancouver: IEEE, 2021. 1–6. [doi: 10.1109/INFOCOMWKSHPS51825.2021.9484510]

[46] Dwork C. Differential privacy. In: Bugliesi M, Preneel B, Sassone V, Wegener I, eds. Proc. of the 2006 Int'l Conf. on Automata, Languages and Programming (ICALP 2006). Venice: Springer, 2006. 1–12. [doi: 10.1007/11787006_1]

[47] McSherry F, Talwar K. Mechanism design via differential privacy. In: Proc. of the 48th Annual IEEE Symp. on Foundations of Computer Science (FOCS 2007). Providence: IEEE, 2007. 94–103. [doi: 10.1109/FOCS.2007.66]

[48] Xu YB, Yang YJ, Han JY, Wang E, Zhuang FZ, Yang JY, Xiong H. NeuO: Exploiting the sentimental bias between ratings and reviews with neural networks. Neural Networks, 2019, 111: 77–88. [doi: 10.1016/j.neunet.2018.12.011]

[49] Lathia N, Hailes S, Capra L, Amatriain X. Temporal diversity in recommender systems. In: Proc. the 33rd Int'l ACM SIGIR Conf. on Research and Development in Information Retrieval. Geneva: ACM, 2010. 210–217. [doi: 10.1145/1835449.1835486]

附中文参考文献:

[22] 葛尧, 陈松灿. 面向推荐系统的图卷积网络. 软件学报, 2020, 31(4): 1101–1112. http://www.jos.org.cn/1000-9825/5928.htm [doi: 10.13328/j.cnki.jos.005928]

[25] 李琳, 刘锦行, 孟祥福, 苏畅, 李鑫, 钟珞. 融合评分矩阵与评论文本的商品推荐模型, 计算机学报, 2018, 41(7): 1559–1573. [doi: 10.11897/SP.J.1016.2018.01559]

[28] 冯兴杰, 曾云泽. 基于评分矩阵与评论文本的深度推荐模型. 计算机学报, 2020, 43(5): 884–900. [doi: 10.11897/SP.J.1016.2020.00884]

© 中国科学院软件研究所 http://www.jos.org.cn

[35] 何明, 常盟盟, 吴小飞. 一种基于差分隐私保护的协同过滤推荐方法. 计算机研究与发展, 2017, 54(7): 1439–1451. [doi: 10.7544/issn1000-1239.2017.20160207]

[42] 刘国丽, 李昂, 李艳萍, 于丽梅. 跨系统协同过滤推荐算法的隐私保护技术研究. 计算机应用研究, 2017, 34(9): 2804–2807. [doi: 10.3969/j.issn.1001-3695.2017.09.053]

王利娥(1981－), 女, 博士, 教授, CCF 专业会员, 主要研究领域为网络与信息安全, 推荐系统, 机器学习.

李先贤(1969－), 男, 教授, 博士生导师, CCF 专业会员, 主要研究领域为数据安全, 分布式系统安全, 可信软件.

李东城(1995－), 男, 硕士, CCF 专业会员, 主要研究领域为网络与信息安全, 机器学习.

© 中国科学院软件研究所 http://www.jos.org.cn