一种基于差分隐私和时序的推荐系统模型研究

范利云[1,2],左万利[1,2],王 英[1,2],王 鑫[3]
(1. 吉林大学计算机科学与技术学院,吉林长春 130012;
2. 吉林大学符号计算与知识工程教育部重点实验室,吉林长春 130012;
3. 长春工程学院计算机技术与工程学院,吉林长春 130012)

摘 要: 推荐系统的建立依赖用户的个人隐私信息,攻击者可以通过推荐的结果对用户的状态和行为进行预测. 目前,虽然有对基于协同过滤近邻隐私保护的研究,但是对基于模型的隐私保护的关注度并不够高. 差分隐私理论定义了一个相当严格的防攻击模型,通过添加噪声使数据失真达到隐私保护的目的,而且用户的兴趣存在兴趣漂移问题,对推荐效果造成影响,因此,提出基于差分隐私理论和时序理论构建基于模型的推荐系统. 首先,根据差分隐私理论,给用户的评分数据增加小波动的符合 Laplace 分布的噪声,增大待分解矩阵的安全系数;然后,在随机梯度下降模型的基础上,将时序因子建模为时间权重,提高模型的准确性. 实验证明该算法的准确性,并且为增强隐私研究提供了新的思路.

关键词: 推荐系统; 非负矩阵分解; 随机梯度下降法; 差分隐私; 时序理论
中图分类号: TP18 **文献标识码:** A **文章编号:** 0372-2112 (2017)09-2057-08
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.09.001

Research on Recommender System Model Based on Differential Privacy and Time Series

FAN Li-yun[1,2], ZUO Wan-li[1,2], WANG Ying[1,2], WANG Xin[3]
(1. *College of Computer Science and Technology, Jilin University, Changchun, Jilin* 130012, *China*;
2. *Key Laboratory of Symbolic Computation and Knowledge Engineering of Ministry of Education, Jilin University, Changchun, Jilin* 130012, *China*;
3. *School of Computer Technology and Engineering, Changchun Institute of Technology, Changchun, Jilin* 130012, *China*)

Abstract: Recommender system is established on users' private information. However, based on results of recommender system, attackers can predict users' states and behaviors. At present, although some researchers are focusing on collaborative filtering neighbor theory to preserve users' privacy, very few researchers pay enough attention to the model-based of privacy-preserving. Differential privacy offers a strong degree of privacy protection by adding noise. And there is interest drift in users' interest. So this paper proposes a recommender system model based on differential privacy theory and time series theory. Firstly, according to differential privacy theory, we add some Laplace-distribution-fitted noises into users' score data to enlarge safety factor in factorization matrix. Then based on stochastic gradient descent model, we model time series factor as time weight to improve the accuracy of the model. Experimental results demonstrate the accuracy of the algorithm, which provides a valuable perspective for privacy-preserving recommender research.

Key words: recommender system; non-negative matrix factorization; stochastic gradient descent; differential privacy; time series

收稿日期 2016-04-11;修回日期:2017-02-14;责任编辑:梅志强
基金项目:国家自然科学基金(No. 60973040, No. 61300148, No. 61602057);吉林省科技发展计划(No. 20130206051GX, No. 20130522112JH, No. 20170520059JH)

1 引言

在过去十年中,推荐系统已经成为网络服务系统中不可替代的一种工具,隐私和安全是所有推荐系统不可避免的问题,如 2010 年 Netfix prize 比赛因涉及到用户的隐私安全而停止举办. 推荐系统主要存在以下隐私风险:推荐系统的建立依赖用户的个人信息,引起对收集并滥用用户隐私的担忧;用户原始的评分信息,即使匿名也可以通过其他数据来源采用脱匿名技术进行隐私预测[1];另外,即使没有直接获取用户的评分信息,也可能从推荐系统中的其他相关用户那里提取到该用户的评分信息[2],因此,推荐系统的这些固有的隐私风险表明隐私保护的研究具有必要性.

目前,差分隐私应用于推荐系统已经得到广泛关注[3],Mcsherry 等人[4]最先将差分隐私保护方法引入到推荐系统中,他们假设推荐系统是不可信的,攻击者可以通过分析推荐系统的历史数据来推测用户的隐私信息,因此,更多的数据拥有者不愿意将自己的数据提供给数据的分析者,或者在自己的数据中去掉一些信息,或者提供一些虚假信息,数据源的不可靠严重影响了推荐系统等数据挖掘的研究. 差分隐私(Differential Privacy,DP)[5]是 2006 年由 Dwork 提出来的,通过在数据中加入小变化的噪声,对计算结果影响较小,同时使攻击者无法通过观察计算结果来获取用户的个人信息. 差分隐私能够解决传统隐私保护模型的两个缺陷:首先,定义了一个严格的防攻击模型,无需考虑攻击者拥有多少背景知识,假设攻击者已获取除目标记录外的所有记录(即最大背景知识假设),该记录的隐私也不会被披露;其次,对隐私保护水平给出了严谨的定义并提供了量化评估方法.

因此,本文基于差分隐私理论提出高效的推荐系统模型,并在数据集上进行多组对比实验,实验证明,本文构建的模型具有较高的扩展性和准确性. 本文的主要贡献如下:

(1)有效地将推荐系统中的差分隐私理论和时序理论进行结合和量化;

(2)在随机梯度下降推荐模型的基础上,将差分隐私理论构建为模型的安全系数,将时序理论建模为时间权重,最终提出推荐系统优化模型(Differential Privacy Time series Stochastic Gradient Descent,PT-SGD);

(3)在数据集上构建多组对比试验,证明 PT-SGD 模型的高效性,并且对模型中所涉及的参数进行不同量化,分析参数对模型性能的影响.

2 相关工作

推荐系统的描述性定义是 1997 年由 Resnick 和 Varian[6]提出的:利用电子商务平台向用户推荐用户感兴趣的信息服务和决策支持,模拟销售人员引导用户购物的功能,提高用户的网络体验. 目前,推荐系统的方法主要可以分为 3 类:基于内容推荐算法(Content-based Recommender),协同过滤算法(Collaborative Filtering),混合推荐算法(Hybrid Recommender).

基于内容推荐算法的理论主要来自于信息检索和信息过滤,通过用户的浏览信息直接分析内容进行推荐,如文献[7,8],该方法的优势是效果直观,不需要领域知识,但是复杂性不好处理. 协同过滤算法以“用户-项目”评分数据作为数据源,可以分为启发式方法和基于模型的方法:启发式方法,通过学习用户(或项目)之间的相似度,提取最近邻用户(或项目),然后基于相似度定量分析模型进行预测,如文献[9,10];基于模型的方法,利用概率模型或机器学习方法进行推荐,主要的模型有矩阵分解模型[11]、概率矩阵分解模型[12]、贝叶斯模型[13],该方法的优势是不需要领域知识,能进行个性化推荐,能处理复杂数据类型,稳定性高,目前已经成为应用最广泛的方法,但是启发式方法具有冷启动问题,即用户评分信息少或没有的时候,无法计算相似用户,基于模型的方法具有解释性差的问题. 混合推荐算法结合上述两种方法,如文献[14],该方法基于图和马尔科夫模型,尽量避免和弥补其他方法的缺点,但是精确度不高.

综合以上相关工作,推荐系统已有较多研究,然而上述方法并没有考虑推荐过程中存在的隐私风险和安全问题.

个性化推荐系统本身固有的隐私风险使增强隐私问题的研究充满了挑战,将之前有关增强用户隐私的推荐系统分成两类:分布式推荐和数据转化技术.

在分布式推荐系统中,用户的相关配置信息被存放在不用的存储设备中,Boutet 等人[15]提出双重机制将用户的配置信息分散存储,首先使用模糊处理来隐藏用户的真实信息,然后利用随机传播协议来保证差分隐私在传播过程中的安全,实验结果表明该模型开销比较小,而且具有较高的适应性;Vallet 等人[16]提出通过 MF 技术将用户信息存储在客户端,使服务器在不保留用户信息的前提下提供精确的推荐. 数据转化技术,Nikolaenko 等人[17]提出数据加密,利用 MF 进行多方面安全计算,推荐系统学习项目代替对评分的学习;Berkovsky 等人[18]提出模糊处理,使用数据模糊策略和协同过滤方法加强隐私;Zhu 等人[19]通过差分隐私理论,实现基于用户协同过滤的差分隐私和基于项目协同过滤的差分隐私,但是没有考虑时间因素.

基于时序的推荐系统将时序信息加入到模型中,使模型能够动态地跟踪用户的兴趣变化,解决兴趣漂

移问题,从而优化推荐效果. Koren 等人[20]提出在奇异值分解算法(Singular Value Decomposition)中加入时序信息,有效解决了兴趣漂移问题;Xiong 等人[21]将时序信息作为第三个维度,然后通过张量分解方法追踪用户兴趣的动态变化;Koshneshin 等人[22]通过演化联合聚类(Evolutionary co-Clustering)算法将用户(产品)动态地分配给不用的聚类,从而做进一步的推荐.

综合以上隐私问题相关研究,尽管已取得一定进展,但是部分模型比较复杂,空间开销比较大,或者牺牲算法精确度来增强隐私的保护,或者没有考虑兴趣漂移对算法性能的影响,这正是本文研究的重点和主要贡献. 本文综合考虑相关研究的各个因素,基于差分隐私理论使输入扰动产生最佳的推荐效果,保证了隐私的稳定水平,同时结合时序理论,追踪用户兴趣的变化,提高推荐的准确性,最终提出构建高效的推荐系统 PT-SGD 模型.

3　推荐系统模型框架

在复杂网络中,隐私问题不仅面临个人隐私信息泄露,还在于基于大数据对人们状态和行为的预测,因此,本文提出基于改进的差分隐私和时序推荐模型 PT-SGD. 该模型首先对数据集进行处理;然后,基于随机梯度下降模型,对“用户-项目”评分数据增加同时满足 Laplace 分布和 L_1-敏感的小变化扰动,将差分隐私理论构建为模型的安全系数,提出 P-SGD 模型;接下来,基于时序理论,将时间衰减函数建模为评分数据的时间权重,跟踪用户喜好的变化;最后,在 P-SGD 模型的基础上,进一步构建 PT-SGD 模型,得到用户和项目矩阵完成预测,基本框架如图 1 所示.

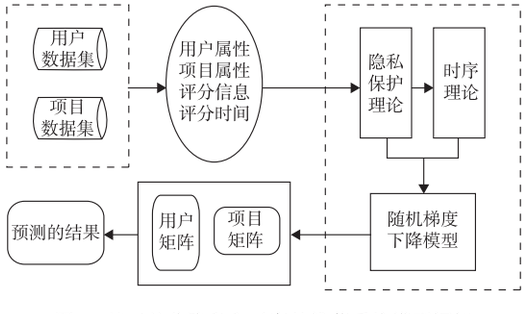

图1　基于差分隐私和时序的推荐系统模型框架

4　数据分析和推荐构建因素量化

4.1　数据分析

数据表达形式为:〈user-ID,item-ID,Rating,Time〉,其中 user-ID 表示用户编号,item-ID 表示项目的唯一标识,Rating 表示 user 对 item 的评分,取值范围为{1,2,3,4,5},Time 表示时间戳,自 1970 年 1 月 1 日数据集产生时刻开始的秒数. 数据矩阵记为 $\boldsymbol{T}$,其格式如下:

$$\boldsymbol{T}=\begin{pmatrix}1 & 1 & 5 & 874965758\\ 56 & 78 & 3 & 892910554\\ 1103 & 1676 & 1 & 1042296388\\ 1137 & 1287 & 4 & 982911558\end{pmatrix}$$

用户集合 $U=\{u_1,u_2,\cdots,u_n\}$ 表示包含 n 个用户,项目集合 $I=\{i_1,i_2,\cdots,i_m\}$ 表示包含 m 个项目,本文将 U 和 I 处理成评分矩阵 $\boldsymbol{R}\in\mathbb{R}^{n\times m}$,以 $\boldsymbol{R}$ 作为模型的输入数据,其中 r_{ui} 表示用户 u 对项目 i 的评分. 矩阵 $\boldsymbol{R}$ 格式如下:

$$\boldsymbol{R}=\begin{pmatrix}r_{11} & r_{12} & \cdots & r_{1m}\\ r_{21} & r_{22} & \cdots & r_{2m}\\ \vdots & \vdots & \ddots & \vdots\\ r_{n1} & r_{n2} & \cdots & r_{nm}\end{pmatrix}$$

4.2　差分隐私因素量化

差分隐私[5,23]的目的是在数据集上提供方法加密用户个人的隐私,同时保证聚类级别信息的准确提取,它是建立在模型的输出不能涉及模型输入的任意特定记录的原则上.

定义 1　差分隐私,我们称随机算法 $K(\varepsilon,\delta)$ 是差分隐私,如果所有的测试集 $S\subset\mathrm{Range}(K)$,$\forall A,B\in\mathbb{R}^n$ 并且 A 和 B 只有一个元素不同,其他的元素都相同,记 $A\approx B$,满足式(1):

$$P(K(A)\in S)\leqslant\exp(\varepsilon)P(K(B)\in S)+\delta \tag{1}$$

如果 $\delta=0$,我们就称 K 是差分隐私. ε 值越小对应的隐私度越高,设置 ε 的可接受界限是一个悬而未决的问题,在文献[23]中设置 $\varepsilon=\mathrm{Ln}\,2$ 或者 $\varepsilon=\mathrm{Ln}\,3$ 被认为是可接受的隐私范围,Dwork 在文献[24]中提出在某些情况下更高的 ε 可以提供更高的推荐精度.

定义 2 L_1-敏感,获得差分隐私的方法是增加随机噪声,大多数添加噪声的数量由 L_1-敏感决定. 给定函数 g,在测试集单个记录变化的情况下,测量结果的最大可能值,L_1-敏感满足式(2):

$$S_1(g)=\max_{A\approx B}\|g(A)-g(B)\|_1 \tag{2}$$

其中,$\|\cdot\|_1$ 定义为 L_1 范数.

定义 3　Laplace 分布,通过向测试集中加入服从 Laplace 分布的噪声来实现 ε-差分隐私. 记位置参数为 0,尺度参数为 b 的 Laplace 分布为 Laplace(b),那么其概率密度满足式(3):

$$f_b(x|b)=\frac{1}{2b}\exp\left(-\frac{|x|}{b}\right) \tag{3}$$

对于给定函数 $g:A\to R^d$,式(4)满足 ε-差分隐私[25].

$$K(x)=g(x)+\mathrm{Laplace}\left(\frac{S_1(g)}{\varepsilon}\right) \tag{4}$$

例如,函数 $g:\mathrm{COUNT}_c(A)$,表示统计数据集 A 中满足条件 c 的记录的个数,记为 count ,同时满足 L_1-敏

感. 如果改变一个记录,count 改变的最大值是 1,即 $S_1(g)=1$,因此,$K(A)=\text{COUNT}_c(A)+\text{Laplace}\left(\frac{1}{\varepsilon}\right)$,满足 ε-差分隐私.

4.3 时序因素量化

用户的喜好在不同时刻肯定是不同的,随着时间的推移,用户的兴趣也会发生变化,即兴趣漂移. 如果算法无法有效地跟踪用户兴趣的变化,对结果的精确度会造成很大的影响,本文针对数据的时间属性构建一个衰减函数作为时间权重,使之满足最晚评分的函数值最大,最早评分的函数值最小的条件,令用户 u 对所有项目的评分的最晚时间为 $\max(u)$,最早时间为 $\min(u)$,用户 u 对项目 i 的评分是 $\text{Ts}(u,i)$,则用户 u 对项目 i 的评分的时间衰减函数定义为:

$$\xi_{ui}=\begin{cases}1.0,\text{s.t. } \max(u)=\min(u)\\ \exp\left(-\dfrac{\max(u)-\text{Ts}(u,i)}{\max(u)-\min(u)}\right),\text{otherwise}\end{cases} \tag{5}$$

当评分 $\text{Ts}(u,i)$ 等于最晚时间 $\max(u)$ 时,时间权重 $\xi_{ui}=\exp(-0.0)=1$,当 $\text{Ts}(u,i)$ 等于最早时间 $\min(u)$ 时,时间权重 $\xi_{ui}=\exp(-1.0)=0.368$,因此,时间权重不仅能够反应用户当前的偏好,也能有效地找出用户目前的主要兴趣.

5 推荐系统模型及优化算法

基于非负矩阵分解推荐模型,以差分隐私理论作为模型构建的安全系数,将时序因子构建为模型的时间权重,提出基于差分隐私和时序的优化模型 P-SGD 和 PT-SGD.

5.1 非负矩阵分解模型

非负矩阵分解(Non-negative Matrix Factorization,NMF)是近几年应用非常广泛的一种矩阵分解方法,常常对数据施加非负性约束,因其充分考虑各种因素的影响,具有良好的扩展性,被广泛应用于图像处理、人脸识别、商品设定或推荐系统、生物信息等领域. 非负矩阵分解将矩阵 $\boldsymbol{R}$ 分解成隐矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$,该方法相比于最近邻方法具有更高的预测精确度,而且时间复杂度低.

本文以评分矩阵 $\boldsymbol{R}$ 作为模型输入,将评分矩阵分解成低维的矩阵,获取用户和项目的潜在因子,预测评分为 $\hat{r}_{ui}=\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}}$,传统的矩阵分解是使目标函数最优化满足公式:

$$L=\min_{P,Q}\sum_{r_{ui}\in R}(r_{ui}-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}})^2 \tag{6}$$

其中,$\boldsymbol{R}\in\mathbb{R}^{n\times m}$,$\boldsymbol{P}\in\mathbb{R}^{n\times d}$,$\boldsymbol{Q}\in\mathbb{R}^{m\times d}$,$d\ll\min(m,n)$. 当"用户-项目"矩阵非常稀疏时就会出现过拟合(over-fitting)问题,因此根据先验知识增加用户因子向量和项目因子向量的范数达到正则化(regularization)的目的,引入正则化项后目标函数为:

$$L=\min_{P,Q}\sum_{r_{ui}\in R}(r_{ui}-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}})^2+\lambda(\|\boldsymbol{P}_u\|_F^2+\|Q_i\|_F^2) \tag{7}$$

其中,λ 是正则项的权重. 该目标函数是非凸函数,本文使用基于随机梯度下降的优化算法来解决这一问题,将在 5.2 节和 5.3 节具体描述.

5.2 差分隐私推荐模型 P-SGD

为了优化 NMF 推荐模型的非凸目标函数,本文提出结合差分隐私理论和随机梯度下降模型(Stochastic Gradient Descent,SGD)构建一个 P-SGD 推荐模型. SGD 模型是机器学习模型中的一种,因其具有简单,可行性高,收敛速度快等特点,受到越来越多研究人员的青睐. SGD 是一种平滑凸优化算法,损失函数对应训练数据集中的每个样本粒度,解决了梯度下降的收敛速度慢和陷入局部最优的两个问题. 在矩阵分解的过程中使用 SGD 进行优化的传统公式为:

$$\frac{\partial L}{\partial \boldsymbol{P}_u}=-2(r_{ui}-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}})\boldsymbol{Q}_i+2\lambda\boldsymbol{P}_u \tag{8}$$

$$\frac{\partial L}{\partial \boldsymbol{Q}_i}=-2(r_{ui}-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}})\boldsymbol{P}_u+2\lambda\boldsymbol{Q}_i \tag{9}$$

每次迭代更新 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$ 的公式为:

$$\boldsymbol{P}_u\leftarrow\boldsymbol{P}_u+\gamma(e_{ui}\boldsymbol{Q}_i-\lambda\boldsymbol{P}_u) \tag{10}$$

$$\boldsymbol{Q}_i\leftarrow\boldsymbol{Q}_i+\gamma(e_{ui}\boldsymbol{P}_u-\lambda\boldsymbol{Q}_i) \tag{11}$$

$$e_{ui}=r_{ui}-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}} \tag{12}$$

其中,γ 是学习速率,γ 越大迭代下降的速率越快,λ 是正则项的权重.

为了达到增强隐私的目的,基于差分隐私理论,根据式(4),设 $g:r_{ui},r_{ui}$ 是测试数据,满足 L_1-敏感,如果改变一个记录,g 改变的最大值是评分最大值与评分最小值的差,即 $S_1(g)=r_{\max}-r_{\min}$,$K(\boldsymbol{R})=r_{ui}+\text{Laplace}\left(\frac{r_{\max}-r_{\min}}{\varepsilon}\right)$,满足 ε-差分隐私. 因此,模型对传统的迭代过程进行改进,式(12)优化如式(13):

$$e_{ui}=r_{ui}+\text{Laplace}\left(\frac{r_{\max}-r_{\min}}{\varepsilon}\right)-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}} \tag{13}$$

5.3 结合差分隐私和时序的推荐模型 PT-SGD

为了追踪用户的兴趣变化,弥补兴趣漂移给模型推荐质量带来的影响,基于 P-SGD 模型将本文提出的时间衰减函数构建为评分的时间权重,式(13)可被重写为:

$$e_{ui}=\xi_{ui}r_{ui}+\text{Laplace}\left(\frac{r_{\max}-r_{\min}}{\varepsilon}\right)-\boldsymbol{P}_u\boldsymbol{Q}_i^{\mathrm{T}} \tag{14}$$

其中,ξ_{ui} 表示对应评分 r_{ui} 的衰减函数,具体形式如式(5)所示. 综上,本文提出的 PT-SGD 模型如算法 1 所示.

算法 1　PT-SGD

输入:用户-项目矩阵 $\boldsymbol{R}$,正则化参数 λ,学习效率 γ,$\boldsymbol{P}$ 的列数 d,隐私参数 ε,迭代次数 iterations
输出:隐特征矩阵 $\boldsymbol{P}$ 和 $\boldsymbol{Q}$
1. 构建训练集和测试集
2. 初始化隐特征矩阵 $\boldsymbol{P}_{nd}$ 和 $\boldsymbol{Q}_{md}$
3. 根据式(3)计算 Laplace 分布
4. For 每次迭代 Do
5.　For $\boldsymbol{R}$ 中每个评分 Do
6.　根据式(14)计算 e_{ui}
7.　For $\boldsymbol{P}$ 中每一列 Do
8.　根据式(10)更新 $\boldsymbol{P}_{ud}$
9.　根据式(11)更新 $\boldsymbol{Q}_{id}$
10.　End For
11.　End For
12. End For
13. Return $\boldsymbol{P}$ 和 $\boldsymbol{Q}$

6　实验与结果分析

通过实验,回答以下 3 个问题:(1)验证本文所构建模型的有效性和精确性;(2)验证差分隐私因素和时序因素对实验的贡献;(3)通过模型中参数的不同量化,说明参数对推荐预测质量的影响.

6.1　数据集

实验采用 Epinions[1] 和 Movielens[2] 数据集,两个数据集都是从网站上搜集的真实数据. Epinions. com 成立于 1999 年,是著名的商品评论网站,包含用户信息、商品属性以及用户对商品的评分信息,评分范围为{1,2,3,4,5};Movielens 数据集是 2011 年第 2 届国际推荐系统研讨会上公布的,由美国 Minnesota 大学的 GroupLens 研究小组创建并维护,该数据集包括用户信息、电影属性以及用户对电影的评分信息,评分范围为{1,2,3,4,5}. Epinions 数据集和 Movielens 数据集包含的用户和商品的个数如表 1 所示.

表 1　数据集

	用户	项目
Epinions	65,269	175,156
ML-100K	943	1,682
ML-1M	6,040	3,952

其中,ML-100K 和 ML-1M 是数据集 Movielens 的两个子集.

6.2　评估方法

为了测试算法的有效性和准确性,本文使用平均绝对误差 MAE(Mean Absolute Error,MAE)作为衡量算法的标准,它真实地反映了测试集与预测数据的误差,该值越小,表明预测的性能越好.

MAE 的公式如下:

$$\mathrm{MAE} = \frac{\sum_{\boldsymbol{R}} |r_{ui} - \hat{r}_{ui}|}{|\boldsymbol{R}|} \tag{15}$$

其中,r_{ui} 和 $\hat{r}_{ui}$ 分别表示用户 u 对项目 i 的真实评分和预测评分,$|\boldsymbol{R}|$ 表示测试集样本的数目.

为确保实验的可靠性,3 组实验均采用 5 倍交叉验证,即将每个数据集平均分成 5 个子集 $\{S_1, S_2, S_3, S_4, S_5\}$,其中 1 个作为测试集,其余 4 个作为训练集,最后取 5 次实验的平均值作为最终结果.

6.3　推荐算法模型对比效果

实验 1 采用 Epinions 数据集,并与算法 Maximum Margin Matrix Factorization(MMMF)[26]、Probabilistic Matrix Factorization(PMF)[27] 和 Constrained Probabilistic Matrix Factorization(CPMF)[27] 进行对比实验. 实验 2 和实验 3 采用 Movielens 数据集,对模型的参数进行定量分析. 综合两个实验可以说明 P-SGD 和 PT-SGD 模型的适用性.

实验 1　因为 MMMF、PMF 和 CPMF 三种方法都属于矩阵分解方法,本文使用的 SGD 模型也是矩阵分解方法的一种,因此,本组实验是将 MMMF、PMF 和 CPMF 三种方法与本文提出的 P-SGD 模型和 PT-SGD 模型进行对比,实验参数设置 $\lambda = 0.06$,$\gamma = 0.01$,$d = 10$,$\varepsilon = 0.7$,iterations = 34,通过 5 倍交叉验证实验结果如图 2 所示.

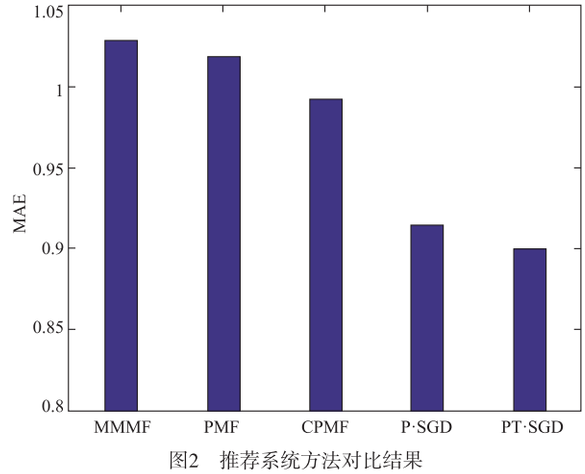

图2　推荐系统方法对比结果

通过实验结果可以看出:

(1) 模型 P-SGD 和模型 PT-SGD 在推荐准确度方面优于其他三种方法,特别是远高于 MMMF,说明模型所增加的差分隐私因子和时序因子对提高模型的推荐质量有一定的促进作用;

(2) 模型 P-SGD 和模型 PT-SGD 对比说明,构建时序因子作为评分的权重优化效果更加明显,有效解决

了兴趣漂移的问题.

综上,本组实验验证了第一个问题和第二个问题.

6.4 模型参数分析

模型 PT-SGD 有两个重要的参数:(1)隐私参数 ε 控制模型的隐私度;(2)迭代次数 iterations 控制模型的精确度. 针对上述的两个问题,本组实验固定一个参数来优化另一个参数,分两部分:(1)ε 的变化对实验的影响;(2) iterations 对模型的影响.

实验 2 在差分隐私中,隐私参数 ε 越小,隐私度越高,设置 $\varepsilon = \mathrm{Ln}\ 2$ 或者 $\varepsilon = \mathrm{Ln}\ 3$ 被认为是可接受的隐私范围,当参数 ε 取值范围为 $\{0.7, 1.7, 2.7, 3.7, 4.7, 5.7, 6.7\}$,$\lambda = 0.06$,$\gamma = 0.01$,$d = 10$,iterations = 10 时,数据集 ML-100K 的实验结果如图 3 所示,图 3(a)是模型 P-SGD 的结果,图 3(b)是模型 PT-SGD 的结果,数据集 ML-1M 的结果类似,限于文章篇幅不再展示.

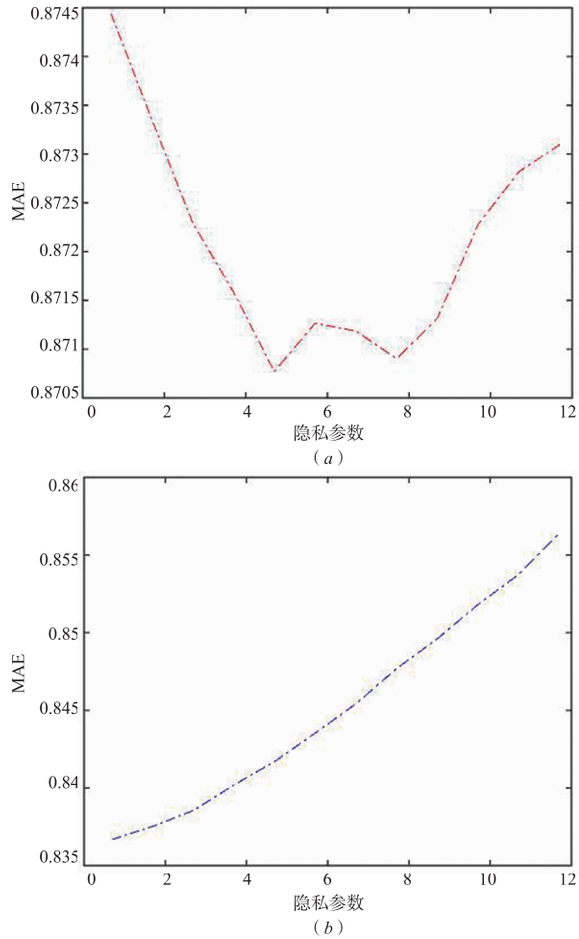

图3 隐私参数对算法性能的影响

通过实验可以看出:

(1) 图 3(a)随着 ε 的增大,ε 在区间[0.7,4.7]上 MAE 逐渐降低,在区间[4.7,7.7]上比较平稳,然后在区间[7.7,11.7]上 MAE 逐渐上升,主要原因是加入过大的噪声对原始数据产生严重的影响,由此可以得出在一定范围内更大的 ε 可以提高推荐的精确度;

(2) 图 3(b)随着 ε 的增大,ε 在区间[0.7,11.7]上 MAE 一直增加,说明 ε 增大没有提高推荐的精确度,也间接的验证了 Dwork 理论的严谨性;

(3) 由于差分隐私理论中隐私参数 ε 值越小隐私度越高,综合(1)、(2)两个结果,通过交叉验证,当 $\varepsilon = 0.07$ 时,PT-SGD 推荐模型的 MAE 精确度最高,故后续的实验中将 ε 设定为 0.7.

综上,本组实验验证了第三个问题.

实验 3 为验证模型 P-SGD 和模型 PT-SGD 在迭代过程中迭代次数 iterations 对实验精确度的影响,本组实验参数设置为 $\lambda = 0.06$,$\gamma = 0.01$,$d = 10$,$\varepsilon = 0.07$,iterations 变化的步长是 4,实验结果如图 4 所示,图 4(a)是数据集 ML-100K 的评估结果,iterations 的范围是[10,110],图 4(b)是数据集 ML-1M 的评估结果,由于 ML-1M 数据集大,时间复杂度比 ML-100K 高很多,所以 iterations 的范围是[6,50].

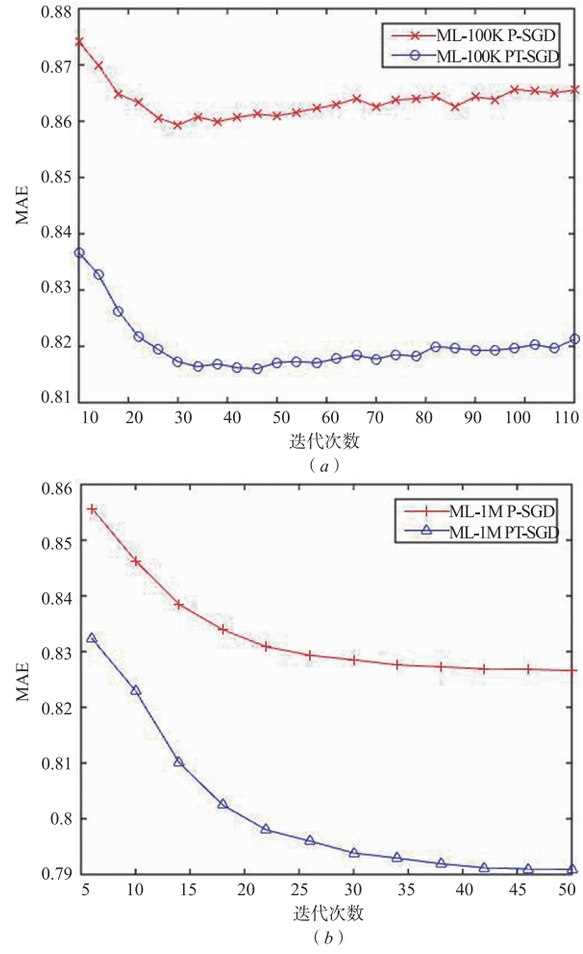

图4 迭代次数对算法性能的影响

通过实验可以看出:

(1)图4(a)数据集 ML-100K,iterations 在区间[30,34]上 P-SGD 和 PT-SGD 达到评估精确度最大值,然后 MAE 有轻微起伏,总体上趋于稳定;

(2) 图4(b)数据集 ML-1M,当 iterations = 34 时,P-SGD 达到评估精确度最大值,当 iterations = 42 时,PT-SGD 达到评估精确度最大值,然后分别趋于稳定;

(3) 其他参数确定的情况下,模型 P-SGD 和模型 PT-SGD 推荐的准确性随着迭代次数 iterations 的增加而逐渐提高,然后趋于稳定;充分说明增加差分隐私因素和时序素对实验推荐质量有重要作用.

综上,本组实验验证了第二个问题和第三个问题.

7　结论和展望

本文在深入研究推荐系统领域的相关技术的基础上,为解决目前推荐系统中亟待解决的增强隐私和兴趣漂移问题,将差分隐私理论构建为模型的安全系数,将时序理论建模为时间权重,提出推荐系统优化模型 PT-SGD,并进行多组对比实验进行验证,实验结果表明,与 MMMF 等方法相比,PT-SGD 模型具有较高的精度.

在今后的工作中,我们将继续探索推荐系统差分隐私理论和其他相关理论,更好地应用到兴趣预测与推荐方面,同时对现有的工作进行优化和改进.

参考文献

[1] Weinsberg U, Bhagat S, Ioannidis S, et al. Blurme: inferring and obfuscating user gender based on ratings[A]. Proceedings of the Sixth ACM Conference on Recommender Systems[C]. Dublin, Ireland: ACM, 2012. 195 – 202.

[2] Calandrino J A, Kilzer A, Narayanan A, et al. " You might also like:" privacy risks of collaborative filtering[A]. Proceedings of the 2011 IEEE Symposium on Security and Privacy[C]. Washington, DC, USA: IEEE, 2011. 231 – 246.

[3] 熊平,朱天清,王晓峰. 差分隐私保护及其应用[J]. 计算机学报,2014,37(1):101 – 122.
Xiong P, Zhu T Q, Wang X F. A survey on differential privacy and applications[J]. Chinese Journal of Computers, 2014, 37(1): 101 – 122. (in Chinese)

[4] Mcsherry F, Mironov I. Differentially private recommender systems: building privacy into the net[A]. Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining [C]. Paris, France: ACM, 2009. 627 – 636.

[5] Dwork C. Differential privacy[A]. Proceedings of the 33rd International Conference on Automata, Languages and Programming[C]. Venice, Italy: Springer, 2006. 1 – 12.

[6] Resnick P, Varian H R. Recommender systems[J]. Communications of the ACM, 1997, 40(3): 56 – 58.

[7] Bogers T, Koolen M. Second workshop on new trends in content-based recommender systems (CBRecSys 2015) [A]. Proceedings of the 9th ACM Conference on Recommender Systems [C]. Vienna, Austria: ACM, 2015. 339 – 340.

[8] Bogers T, Koolen M. Report on RecSys 2015 workshop on new trends in content-based recommender systems[J]. ACM SIGIR Forum, 2016, 49(2): 141 – 146.

[9] Anava O, Golan S, Golbandi N, et al. Budget-constrained item cold-start handling in collaborative filtering recommenders via optimal design[A]. Proceedings of the 24th International Conference on World Wide Web [C]. Florence, Italy: ACM, 2015. 45 – 54.

[10] Jiang X, Liu W, Cao L, et al. Coupled collaborative filtering for context-aware recommendation[A]. Proceedings of the Twenty-Ninth AAAI Conference on Artificial Intelligence [C]. Texas, USA: AAAI, 2015. 4172 – 4173.

[11] Liu Z, Wang Y X, Smola A. Fast differentially private matrix factorization[A]. Proceedings of the 9th ACM Conference on Recommender Systems[C]. Vienna, Austria: ACM, 2015. 171 – 178.

[12] 印桂生,张亚楠,董宇欣,等. 基于受限信任关系和概率分解矩阵的推荐[J]. 电子学报,2013,42(5):904 – 911.
Yin G S, Zhang Y N, Dong Y X, et al. A constrained trust recommendation using probabilistic matrix factorization [J]. Acta Electronica Sinica, 2013, 42(5): 904 – 911. (in Chinese)

[13] Zhang W, Wang J. A collective bayesian poisson factorization model for cold-start local event recommendation[A]. Proceedings of the 21th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining[C]. Sydney, Australia: ACM, 2015. 1455 – 1464. .

[14] Kouki P, Fakhraei S, Foulds J, et al. HyPER: A flexible and extensible probabilistic framework for hybrid recommender systems[A]. Proceedings of the 9th ACM Conference on Recommender Systems [C]. Vienna, Austria: ACM, 2015. 99 – 106.

[15] Boutet A, Frey D, Guerraoui R, et al. Privacy-preserving distributed collaborative filtering[A]. Proceedings of the Second International Conference, NETYS 2014[C]. Marrakech, Morocco: Springer, 2014. 169 – 184.

[16] Vallet D, Friedman A, Berkovsky S. Matrix factorization without user data retention[A]. Proceedings of the 18th Pacific-Asia Conference on Knowledge Discovery and Data Mining [C]. Tainan, Taiwan: Springer, 2014. 569 – 580.

[17] Nikolaenko V, Ioannidis S, Weinsberg U, et al. Privacy-

preserving matrix factorization[A]. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security[C]. Berlin, Germany: ACM, 2013. 801 – 812.

[18] Berkovsky S, Kuflik T, Ricci F. The impact of data obfuscation on the accuracy of collaborative filtering[J]. Expert Systems with Applications, 2012, 39(5): 5033 – 5042.

[19] Zhu X, Sun Y. Differential privacy for collaborative filtering recommender algorithm[A]. Proceedings of the 2016 ACM on International Workshop on Security And Privacy Analytics[C]. New Orleans, Louisiana, USA: ACM, 2016. 9 – 16.

[20] Koren Y. Collaborative filtering with temporal dynamics. Commun ACM[J]. Communications of the ACM, 2010, 53(4): 89 – 97.

[21] Xiong L, Chen X, Huang T, et al. Temporal collaborative filtering with bayesian probabilistic tensor factorization[A]. Proceedings of the 2010 SIAM International Conference on Data Mining[C]. Columbus, Ohio, USA: DBLP, 2010. 211 – 222.

[22] Khoshneshin M, Street W N. Incremental collaborative filtering via evolutionary co-clustering[A]. Proceedings of the Fourth ACM Conference on Recommender systems[C]. Barcelona, Spain: ACM, 2010. 325 – 328.

[23] Dwork C, Mcsherry F, Nissim K. Calibrating noise to sensitivity in private data analysis[A]. Proceedings of the Third Conference on Theory of Cryptography[C]. New York, USA: Springer, 2006. 265 – 284.

[24] Dwork C. Differential privacy: A survey of results[A]. Proceedings of the 5th International Conference on Theory and Applications of Models of Computation[C]. Xian, China: Springer, 2008. 1 – 19.

[25] Berlioz A, Friedman A, Kaafar M A, et al. Applying differential privacy to matrix factorization[A]. Proceedings of the 9th ACM Conference on Recommender Systems[C]. Vienna, Austria: ACM, 2015. 107 – 114.

[26] Rennie J D M, Srebro N. Fast maximum margin matrix factorization for collaborative prediction[A]. Proceedings of the 22nd International Conference on Machine Learning[C]. Bonn, Germany: ACM, 2005. 713 – 719.

[27] Salakhutdinov R, Mnih A. Probabilistic matrix factorization[A]. Proceedings of Advances in Neural Information Processing Systems[C]. Vancouver, Canada: NIPS, 2007. 1257 – 1264.

作者简介

范利云 女,1990 年出生,河南安阳人,现为吉林大学计算机科学与技术学院硕士研究生,从事机器学习、数据挖掘等有关研究.
E-mail: fanlyjlu@163.com

左万利(通信作者) 男,1957 年出生,吉林吉林人,博士,现为吉林大学计算机科学与技术学院教授、博士生导师,从事数据库、Web 智能、搜索引擎、自然语言处理等有关研究.
E-mail: wanli@jlu.edu.cn