Computer Science and Application 计算机科学与应用, 2020, 10(3), 427-436
Published Online March 2020 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2020.103044

Hans汉斯

Privacy Protection Based on the Publication of Recommended Social Media Data

Xinglan Zhang, Jie Yang

Beijing University of Technology, Beijing
Email: 1374666209@qq.com

Received: Feb. 16th, 2020; accepted: Mar. 2nd, 2020; published: Mar. 9th, 2020

Abstract

Personalized recommendation requires the use of a large amount of user data, especially the activity data of users on social media, including ratings, check-ins, etc. However, from a large amount of user activity data, users' privacy data can be inferred. In this paper, aiming at the characteristics of FM recommendation algorithm, distance measurement KFC (Kendall feature correlation) was proposed to constrain data distortion, and PrivFM, a customizable, continuous and privacyprotecting social media data publishing framework, was proposed to prevent inference attacks by disrupting the active data published by users, while ensuring the recommendation effectiveness. The experimental results show that compared with other privacy protection methods and distance measurement, the balance between privacy protection and recommendation is improved.

Keywords

Privacy Protection, Data Publishing, FM Based Recommendation, Social Media

基于推荐的社交媒体数据发布的隐私保护

张兴兰，杨　捷

北京工业大学，北京
Email: 1374666209@qq.com

收稿日期：2020年2月16日；录用日期：2020年3月2日；发布日期：2020年3月9日

摘　要

个性化的推荐需要使用大量的用户数据，尤其是用户在社交媒体上的活动数据，包括评级、签到等，然而，从大量的用户活动数据中，能够推断出用户的隐私数据。在本文中，针对FM推荐算法的特性，提出

文章引用: 张兴兰, 杨捷. 基于推荐的社交媒体数据发布的隐私保护[J]. 计算机科学与应用, 2020, 10(3): 427-436.
DOI: 10.12677/csa.2020.103044

距离度量KFC，约束数据失真，提出了PrivFM，一个可定制的、连续的、保护隐私的社交媒体数据发布框架，通过扰乱用户发布的活动数据，防止推理攻击，同时保证推荐效用。实验结果表明，相对于其他的隐私保护方法及距离度量，提高了隐私保护与推荐之间的平衡。

关键词

隐私保护，数据发布，基于FM推荐，社交媒体

1. 引言

随着信息技术特别是互联网、物联网和云计算等技术的迅猛发展，网络空间中所蕴含的信息量呈指数级增长。信息过载现象愈发严重，给人们带来很大的信息负担。推荐系统作为一种有效的信息过滤手段是当前解决信息过载问题及实现个性化信息服务的有效方法之一。为了提供高质量和个性化的推荐，推荐系统需要收集大量的用户信息、用户行为等，尤其是社交媒体上的用户活动数据，例如标记/评级记录、评论、登记或其他类型的数据。在实践中，许多用户愿意将他们在社交媒体上的在线活动的数据(或数据流)发布给服务提供商，以获得高质量的个性化推荐。然而，他们通常认为来自社交媒体的部分数据是私人的，例如性别、收入水平、政治观点或社会交往等。虽然用户可能拒绝发布私有数据，但公共数据和私有数据之间的内在关联往往会导致严重的隐私泄漏。例如，一个人的政治归属可以从对电视节目的评价中推断出来[1]；一个人的性别可以从社交网络上的位置活动数据中推断出来[2]。这些研究表明，私有数据经常遭受推理攻击[3]，敌人通过分析用户的公共数据以非法获取有关其私有数据。因此，在将公共数据发布到推荐系统时，保护用户私有数据至关重要。

为了解决这一问题，保护隐私数据的发布平台被广泛研究[4]。它的基本思想是通过在公开数据发布之前对其进行扭曲，以牺牲公共数据在后期处理阶段的效用，来保护私有数据。对于推荐引擎的用例，效用是指基于被扭曲的公共数据的个性化性能，即推荐引擎是否能够根据模糊数据准确预测个人偏好。在隐私和隐私之间存在一种内在的平衡。

差分隐私[5]是一种众所周知的技术，保证用户对具有任意背景知识的攻击者的隐私。在此背景下，还提出了信息论隐私保护方法。他们试图基于各种基于熵的度量(如条件熵[6]和相互信息[7])定量地测量隐私泄漏，并基于这些度量设计隐私保护机制，提出了几种隐私保护信息熵模型[8]。尽管差分隐私的概念与信息论方法相比更为严格，但是后者更直观、更易访问，符合许多应用领域的实际需求。尤其是信息论可以提供直观的指导，通过观察和分析用户的公共数据(即公共数据中的私人数据的隐私泄漏)，定量测量对手可以学习的用户私人信息量。在基于信息论现有的文献中，现有的数据模糊方法主要是通过使用欧几里得距离[9]、肯德尔等级相关系数距离[10]等指标来限定数据失真，从而确保数据的实用性。它们类似于限制对项目预测用户评级的损失，目标是将预测评分和用户实际评分之间的整体差异减少。

这些度量数据失真的方法，只单方面地考虑了失真数据与真实数据的距离，并没有保留数据变换之后，两两特征之间的关联度。而基于因子分解机的推荐技术，主要是使用特征之间的关联进行推荐，因此，本文考虑使用自定义距离 KFC，将数据模糊过程中产生的特征关联度损失进行约束，保留特征之间的关系。

2. 理论基础

本节首先介绍基于因子分解机的推荐算法，然后介绍近年来用于隐私度量的信息熵及其实现机制。

2.1. 因子分解机

因子分解机最初是为了解决类别特征存在较多取值是经过 One-Hot 编码以后数据国语稀疏导致模型学习能力欠佳的问题，同时也解决了线性模型的特征之间无法进行组合的问题，某些特征经过关联以后，与标签之间的关联性会增强。比如有的女生喜欢化妆品，男生喜欢运动产品。单纯的使用 $w_1 * x_1 + w_2 * x_2 + \cdots + w_i * x_i$ 是无法实现特征之间的关联的。为了实现特征之间的组合，可以在线性的基础上引入二次项：

$$y = w_0 + \sum_{i=1}^{n} w_i * x_i + \sum_{i=1}^{n}\sum_{j=1}^{n} w_{ij} * x_i x_j \tag{1}$$

n 为一个样本的特征个数。 w_{ij} 为特征 x_i 和 x_j 之间的因子，共有 $n(n-1)/2$ 个。

在数据进行训练之前，都会进行 One-Hot 编码，这样在编码之后数据的维度会特别大，而且会存在大量的 0。这样的稀疏矩阵对于求解上面 w_{ij} 是非常不利的。因此对于每一个特征可以引入一个辅助向量 v_i，使其满足 $w_i = v_i v_j^{\mathrm{T}}$ 其中 $v_i = (v_{i1}, v_{i2}, \cdots, v_{ik})$，因此式(1)可以写成：

$$y = w_0 + \sum_{i=1}^{n} w_i * x_i + \sum_{i=1}^{n}\sum_{j=1}^{n} \langle v_i v_j \rangle * x_i x_j \tag{2}$$

通过矩阵对称性化简等式(2)为：

$$y = w_0 + \sum_{i=1}^{n} w_i * x_i + \frac{1}{2}\sum_{f=1}^{k}[(\sum_{i=1}^{n} v_{i,f} x_i)^2 - \sum_{i=1}^{n} v_{i,f}{}^2 x_i^2] \tag{3}$$

使得时间复杂度从 $O(kn^2)$ 降低为 $o(kn)$。因此，在特征数量急剧膨胀导致计算量陡增的背景下，因子分解机是一种十分高效的模型。

2.2. 推理攻击

假定攻击者使用方法 q 来推断出 y (y 为隐私数据)，并且攻击者总是试图使用 q 推到出 y 的代价(c)最小，以此来得到方法 q。

$$c = \min_{q} E_Y\left[C(Y,q)\right] \tag{4}$$

其中 $C(Y,q)$ 是使用 q 推导出 y 的预期成本函数。发布数据 x 进行数据混淆，得到数据 x，通过解决以下问题，可以得到 q。

$$\hat{c} = \min_{q} E_{Y|\hat{x}}\left[C(Y,q)|\hat{X}\right] \tag{5}$$

攻击者在观察混淆数据 $\hat{x}$ 后的成本收益为：

$$\Delta C = c - \hat{c} \tag{6}$$

ΔC 表示敌手在观察 $\hat{x}$ 后，获取的隐私代价。隐私保护的理念是，找到 $\hat{x}$，使 ΔC 最小，并且能够使用 $\hat{x}$ 进行推荐。

3. 框架流程

为应对基于用户隐私的推理攻击，设计了基于隐私保护服务器的推荐系统架构(PriFM)。整个系统架构主要由用户、数据发布平台、第三方服务器三部分组成。推荐及隐私保护过程如下：

1) 首先用户将自己的活动数据上传到社交网站，尤其是标签、评分、评论等能够反映个人偏好的活动。当用户想要订阅第三方服务时，授予第三方访问此类活动数据的权限，得到第三方的服务。

2) 根据用户自己的隐私标准，数据发布平台对其历史活动数据进行模糊处理，以保护用户指定的私有数据不受推理攻击。当用户在社交媒体上连续报告其活动时，在线数据发布模块在将其活动流发送到第三方服务之前，对其活动流中的每个活动进行模糊处理。所有的数据混淆都是在保证个性化的基于因子分解机的推荐的效用下进行的，通过限制混淆数据引起的特征关联度损失。

3) 尽管第三方服务接收到模糊的公共数据，但仍然可以向用户提供高质量的基于因子分解机的推荐。

4. 历史数据发布

首先，为了减少学习最佳混淆函数所产生的问题复杂性，在框架中结合聚类算法。由于类似的用户活动常常引起类似的隐私泄漏[11]，因此，使用公共数据将类似用户聚集到一个组，将大量用户分为有限的数组集合。然后，基于用户聚类，从公共数据中定量地测量用户指定的私有数据(如性别)的隐私泄漏，在给定的失真预算下通过最小化隐私泄漏来学习最优模糊函数，并且限制特征关联度的损失。最后，基于所学习的模糊函数，进行概率数据模糊处理。

4.1. 用户聚类

从每一个用户的公共数据中直接学习最优混淆函数 $P_{\hat{x}|x}$，会导致复杂度按用户的数量的二次增长。为了减少问题的复杂性，用户聚类阶段根据用户的公共数据向量将用户聚类成有限数量和固定数量的组。我们根据用户的历史记录对用户集进行聚类，为了简单起见，采用欧氏距离的层次聚类，根据聚类结果，我们得到了用户 U 到聚类 G 的映射，其中每个元素 g ($g \in G$)是对应聚类的质心。

4.2. 聚类模糊函数学习

4.2.1. 信息熵隐私度量

隐私泄露通过攻击者在观察混淆数据以后，产生的信息增益 ΔC 来测量。Calmon 等人[12]证明了 ΔC 可以表示为混淆数据与隐私数据之间的互信息。

$$\Delta c = I\left(\hat{X},Y\right) = \sum_{\hat{x}\in\hat{X},y\in Y} p\left(\hat{x},y\right)\log\frac{p\left(\hat{x},y\right)}{p\left(\hat{x}\right)p\left(y\right)} \tag{7}$$

如上所述，我们使用概率模糊函数 $p_{\hat{X}|X}$ 生成发布的混淆数据 $\hat{x}$，因此，联合概率 $\hat{x}$ 和 y 可以通过下面来计算：

$$p\left(\hat{x},y\right) = \sum_{x\in X} p_{\hat{X}|X}\left(\hat{x}\,|\,x\right)p_{X,Y}\left(x,y\right) \tag{8}$$

边际概率 $p_{\hat{X}}\left(\hat{x}\right), p_X\left(x\right), p_Y\left(y\right)$ 可以通过以下计算：

$$p_{\hat{x}}\left(\hat{x}\right) = \sum_{x\in X,y\in Y} p_{\hat{x}|x}\left(\hat{x}\,|\,x\right)p_{X,Y}\left(x,y\right) \tag{9}$$

$$p_X\left(x\right) = \sum_{y\in Y} p_{X,Y}\left(x,y\right), p_X\left(y\right) = \sum_{x\in X} p_{X,Y}\left(x,y\right) \tag{10}$$

结合上述公式，发布公共数据 $\hat{x}$ 和隐私数据 y 可以描述为：

$$I\left(\hat{X},Y\right) = \sum_{\hat{x}\in\hat{X},y\in Y} p\left(\hat{x},y\right)\log\frac{p\left(\hat{x},y\right)}{p\left(\hat{x}\right)} - \sum_{y\in Y} p\left(y\right)\log p\left(y\right) \tag{11}$$

其中第二项是 y 的熵，即为给定数据集中指定隐私数据的常量。因此，在互信息中，忽略此项，得到：

$$I\left(\hat{X},Y\right)=\sum_{\hat{x}\in\hat{X},y\in Y}p\left(\hat{x},y\right)\log\frac{p\left(\hat{x},y\right)}{p\left(\hat{x}\right)} \tag{12}$$

结合公式(8)和(9)，互信息可以只描述为两个因素，使用给定的数据集产生的 $p_{X,Y}$ 和混淆函数 $P_{\hat{X}|X}$：

$$I\left(\hat{X},Y\right)=\sum_{\hat{x}\in\hat{X},x\in X,y\in Y}p_{\hat{X}|X}\left(\hat{x}\mid x\right)p_{X,Y}\left(x,y\right)*\log\frac{\sum_{x'\in X}p_{\hat{X}|X}\left(\hat{x}\mid x'\right)p_{X,Y}\left(x',y\right)}{\sum_{x''\in X,y'\in Y}p_{\hat{X}|X}\left(\hat{x}\mid x''\right)p_{X,Y}\left(x'',y'\right)} \tag{13}$$

$P_{\hat{X}|X}$ 在给定的失真约束 Δx，通过最小化 $I\left(\hat{X},Y\right)$ 取得。

4.2.2. 距离度量

基于因子分解机的推荐算法主要是利用两两特征组合，引入交叉项特征，提高模型得分，因此对数据混淆过程中产生的两两特征间关联度损失非常敏感。因此，不能使用其他类型的损失来衡量，如欧几里德、平方 L2、肯德尔等级相关系数来衡量。表 1 为项目评分特征关联损失的实例，原始评分模糊为 b 或者 c，当两个模糊数据的欧式距离完全相同时，所产生的特征关联损失不同。b 两两特征间的差异与 a 相同，没有产生任何特征关联度损失，c 则产生的特征关联度损失为 5 (设 $\varepsilon=1$)，表明相同的数据失真预算用欧几里德距离意味着不同的特征关联度的损失。因此，考虑到数据造成的特征关联度损失模糊处理对于因子分解机推荐算法至关重要，我们定义一种类似于肯德尔等级相关系数距离——KFC，用来衡量两个列表之间的成对关联度不一致的数量。对于两个用户 A 和 B，分别将其公共数据向量表示为 v^a 和 v^b，则距离 $KFC\left(v^a,v^b\right)$ 的计算方式为：

$$KFC\left(V^a,V^b\right)=\sum_{i,j}I_{\left|\left(V_i^b-V_j^b\right)-\left(V_i^a-V_j^a\right)\right|>\varepsilon} \tag{14}$$

V_i^a 为列表 v_a 中项目 i 的项目得分，依次类推。I_{cond} 是一个指示函数，当 I_{cond} 为真时，等于 1，否则等于 0。ε 为允许两两特征关联度差异的最大值，区间为[0, t]，t 为项目评分的最大值。将等式计算出的成对关联度不一致的数量除以 $n\left(n-1\right)/2$，标准化到[0,1]区间，值为 1 表示最大不一致，值为 0 表示两个列表有相同的特征关联度，则：

$$KFC\left(V^a,V^b\right)=\frac{1}{n\left(n-1\right)/2}\sum_{i,j}I_{\left|\left(V_i^b-V_j^b\right)-\left(V_i^a-V_j^a\right)\right|>\varepsilon} \tag{15}$$

在实践中，当有 n 维特征时，计算两两特征之间的关联度距离，需要进行 $n\left(n-1\right)/2$ 次的成对比较，得到的计算复杂度为 $O\left(n^2\right)$。为了提高计算效率，我们使用自举采样来近似计算特征间的关联度，并不比较所有特征对之间的关联度，而是随机抽取 S 对特征进行比较，在统计 S 对特征关联度之后，通过除以 $\left|S\right|$ 将其规范化：

$$KFC\left(V^a,V^b\right)=\frac{1}{\left|S\right|}\sum_{(i,j)\in S}I_{\left|\left(V_i^b-V_j^b\right)-\left(V_i^a-V_j^a\right)\right|>\varepsilon} \tag{16}$$

Table 1. Data before and after project scoring confusion
表 1. 项目评分混淆前后数据

项目	i	j	k	g
原始评分 a	1	2	3	4
混淆评分 b	2	3	4	5
混淆评分 c	3	2	5	4

4.2.3. 模糊函数学习

模糊处理功能是根据单个活动数据进行学习的，其中活动是指项目上的评级、标签等。为了将公共数据 i ($i \in I$)中的私人数据 y 的隐私泄漏降至最低，我们遵循用于群集模糊功能学习的相同隐私实用程序权衡框架，并尝试将 $I\left(\hat{i},Y\right)$ 最小化。为了更好地约束特征关联度损失，我们事先计算两两特征之间的关联度，并进行存储，再基于 Bootstrap 采样近似，来计算总的特征间的关联度。总之，我们首先通过经验计算 $P_{i,Y}$，并使用算法 1 学习每个用户 u 的最优模糊函数 $P^u_{\hat{i}|i,Y}$，这也是一个凸优化问题。

算法 1. 模糊函数学习

输入：联合概率 $P_{i,Y}$，失真预算 Δx，用户公共数据向量 V^u

输出：模糊函数 $p^u_{\hat{i}|i,Y}$

1. 求解最优化问题 $p_{\hat{i}|i}$

2. $$\min_{p_{\hat{i}|i}} I\left(\hat{i}\mid i,Y\right)$$

3. $$\text{s.t.}, E_{\hat{i},i}\left(KFC\left(i,\hat{i}\right)\right)\le \Delta x$$

4. $$p_{\hat{i}|i}\left(\hat{i}\mid i\right)\in[0,1],\forall i,\hat{i}\in I$$

5. $$\sum_{\hat{i}} p_{\hat{i}|i}\left(\hat{i}\mid i\right)=1,\forall i\in I$$

6. 返回模糊函数 $p^u_{\hat{i}|i,Y}$

4.3. 概率在线活动混淆

基于学习到的模糊函数，我们使用算法 2 对来自用户活动流的每个传入活动进行模糊处理。对于项目 i 上的每个传入活动，我们首先获得相应的模糊函数 $P^u_{\hat{i}|i,Y}$ 来保护 u 指定的私有数据 y。然后，我们基于 $P^u_{\hat{i}|i,Y}\left(\hat{i}\mid i\right)$ 对项目 i 上的活动进行模糊处理，并将活动 i 映射为项目 i 上作为模糊数据。

算法 2. 混淆在线活动数据

输入：模糊函数 $p^u_{\hat{i}|i,Y}$，失真预算 Δx，活动数据 i

输出：模糊数据 $\hat{i}$

1. 求解最优化问题 $p_{\hat{i}|i}$

2. $$\min_{p_{\hat{i}|i}} I\left(\hat{i}\mid i,Y\right)$$

3. $$\text{s.t.}, E_{\hat{i},i}\left(K\left(i,\hat{i}\right)\right)\le \Delta x$$

4. $$p_{\hat{i}|i}\left(\hat{i}\mid i\right)\in[0,1],\forall i,\hat{i}\in I$$

5. $$\sum_{\hat{i}} p_{\hat{i}|i}\left(\hat{i}\mid i\right)=1,\forall i\in I$$

6. 返回模糊函数 $p^u_{\hat{i}|i,Y}$

5. 实验结果与分析

5.1. 评价指标

(1) 推荐质量评估

评价推荐系统推荐质量的度量标准主要有统计精度度量方法、决策支持精度度量方法和排名度量方法。本文实验采用统计精度度量方法中均方根误差作为评价指标来衡量评分预测推荐精确度：

$$RMSE = \sqrt{\frac{\sum_{(i,j)\in R}\left(r_{ij} - \hat{r}_{ij}\right)^2}{|R|}}$$

其中，R 表示评测集中的评分矩阵，r_{ij} 表示实际评分，r_{ij} 表示预测评分。RMSE 越小，说明推荐算法的精确度越好，推荐质量越高。

(2) 隐私保护性能评估

对私有数据的推断攻击试图从用户发布的公共数据 $\hat{x}$ 中推断出用户的私有信息 y (例如，性别)，这可视为离散数据的分类问题。因此，我们使用两种推理攻击方法直接评估隐私保护的性能，即支持向量机和朴素贝叶斯。假设敌人已经根据一些非隐私意识用户的原始公共数据 x 和私有数据 y 训练了他们的分类器。我们随机抽取 50%的用户作为非隐私意识用户进行分类训练，然后根据模糊活动数据 $\hat{x}$ 对其余用户的隐私数据 y 进行推理攻击。我们使用曲线下面积(AUC)来评估推理攻击的性能。在实验中，我们将此值(1 - AUC)作为隐私保护指标。较高的(1 - AUC)值意味着更好的隐私保护。当 AUC = 0.5 时，则意味着任何推理攻击方法的性能都不比随机猜测好。

5.2. 数据集

本文采用 GroupLens 研究组提供的 MovieLens 数据集 ML-100k 对算法进行评估，该数据集包含了 943 个用户对 1682 部电影的 100,000 个评分记录，每个用户至少对 20 部电影评 过分，评分范围为 1~5 之间的整数，代表喜好程度从低到高。该数据集的评分稀疏度为 93.7%。实验中，我们将数据集平均分成 5 组，采用交叉验证的方法进行实验，训练集与测试的大小比例为 4:1。

基于公开的数据集，首先研究隐私保护与基于因子分解机推荐性能之间的权衡。其次，与其他隐私保护推荐算法进行对比。最后，探讨了不同损失度量下基于因子分解机推荐的效用保证。

5.3. 实验比较与分析

5.3.1. 隐私保护与效用权衡

使用以下两种方法进行比较：

随机混淆：对于历史数据模糊处理，给定的概率 p，随机模糊每个用户的公共数据向量[13]。p 控制了扭曲预算。

差分隐私：不关心攻击者所具有的背景知识，即使攻击者已经掌握除了一条记录之外的所有记录的敏感信息，该记录的敏感信息也无法被披露[14]。差分隐私有两种实践机制，拉普拉斯机制和指数机制，前者适用于结果为数值型的保护，后者适用于结果为非数值型的保护。在这里，我们使用前者来进行比较。

在这个实验中，我们调整不同方法中的模糊处理预算，以直接显示隐私实用程序的权衡。PriFM 框架的参数主要是控制失真预算。我们将性别是所有实验中的私人数据，为了运行时效率，根据经验，选择用户群的数量 $|G| = 200$ 和对样本的数量 $|S| = 10^4$，$|S|$ 用于估计每个用例的 KFC 距离。

图 1 显示了在电影数据集上不同隐私保护数据模糊处理方法的隐私－效用权衡结果。首先，我们清楚地观察到隐私保护和为所有方法启用基于 FM 的推荐的效用之间的权衡。虽然，高度扭曲的公共数据使得敌人难以推断出用户的私人数据，有更好的隐私保护。但是，高度扭曲的公共数据会导致较高的数据效用损失，也会阻止推荐算法准确预测用户的偏好。其次，我们能够观察到，与其他方法相比，PriFM 始终能够在所有情况下实现更好的隐私保护和更高的效用。

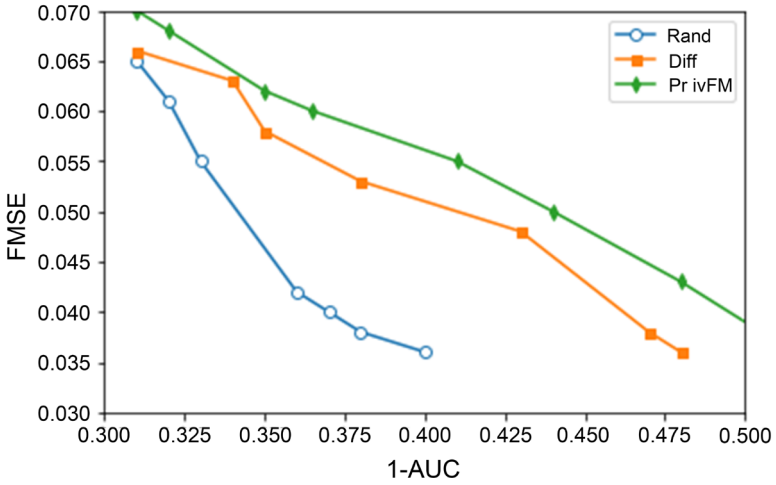

Figure 1. Different approaches to privacy-utility tradeoffs on the movielens-1m dataset
图 1. 不同的方法在 Movielens-1M 数据集上进行隐私-效用权衡

5.3.2. 隐私保护性能

PrivFM 框架旨在保护用户特定的私人数据，在这个实验中，我们将性别作为隐私数据，并报告定制的隐私保护性能。我们调整了所有数据模糊处理方法的失真预算，以保持相同的数据效用。图 2 显示了电影数据集上的性别隐私保护结果。我们观察到，在保护私人性别时，我们的框架优于所有其他方法，因为它实现了 1-AUC 的最高值。这表明，在相同的数据下，个人的隐私可以达致更佳的私隐保障。

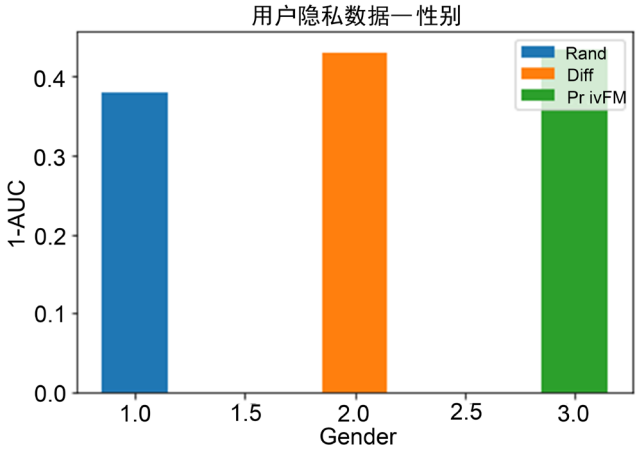

Figure 2. Privacy data-gender measurement
图 2. 隐私数据－性别衡量

5.3.3. 不同损失度量的效用

在本实验中，我们使用我们的方法研究了隐私－效用权衡的不同损失度量，包括欧几里得度量，余弦距离和基于特征损失的度量的 KFC 距离。我们保持其他参数和以前的实验一样。图 3 显示了不同损失指标下的隐私－效用权衡。首先，我们观察到，基于 KFC 的损失指标优于其他两个指标的指标，因为它同时实现了更好的隐私保护和效用。换句话说，限制数据混淆造成的特征关联度损失可以更好地保持公共数据中的特征之间的关系，从而降低学习 FM 算法的效用损失。PriFM 可以有效地提高基于排序的推荐在相同的隐私保护水平下的效用。

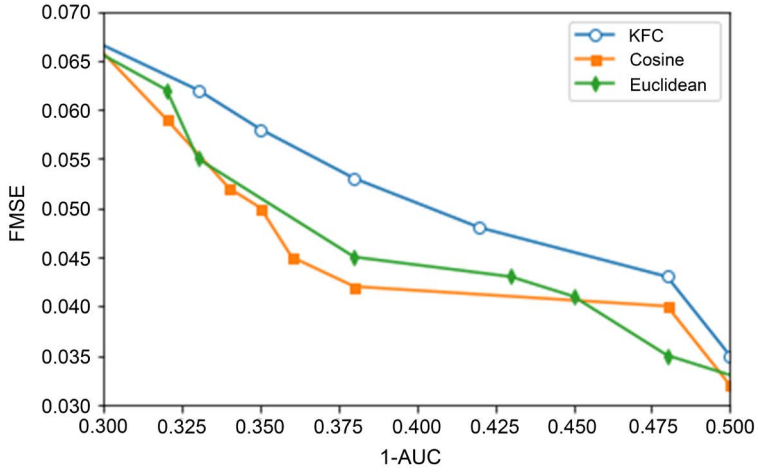

Figure 3. Privacy utility tradeoffs, different distance measures
图 3. 隐私效用权衡——不同距离度量

6. 结束语

本文介绍了一种可定制、连续的隐私保护的社交媒体数据发布框架，通过发布模糊的用户活动数据，不断地保护用户指定的数据免受推理攻击，同时仍然确保所发布数据的实用性，以增强基于因子分解机的推荐。为了提供定制的保护，我们学习了最佳的数据混淆方法，以便将用户指定的私有数据的泄漏降到最低，为了确保数据实用性，减少特征间的关联性的损失，我们使用类似于 Kendall-t 距离来限制数据混淆过程中产生的关联度损失 KFC。我们通过大量实验证明 PriFM 框架可以提供对私有数据的有效保护，同时还可以为基于因子分解机的推荐用例保留已发布数据的效用。如何在隐私保护和推荐质量之间寻找一个平衡是一个值得深入研究的课题。

参考文献

[1] Salamatian, S., Zhang, A., Calmon, F.D.P., Bhamidipati, S., Fawaz, N., Kveton, B., Oliveira, P. and Taft, N. (2013) How to Hide the Elephant- or the Donkey- in the Room: Practical Privacy against Statistical Inference for Large Data. https://doi.org/10.1109/GlobalSIP.2013.6736867

[2] Yang, D., Zhang, D., Qu, B., *et al*. (2016) PrivCheck: Privacy-Preserving Check-in Data Publishing for Personalized Location Based Services. In: *Proceedings of* 2016 *ACM International Joint Conference*, ACM, New York. https://doi.org/10.1145/2971648.2971685

[3] Li, C., Shirani-Mehr, H. and Yang, X.C. (2007) Protecting Individual Information against Inference Attacks in Data Publishing. *Advances in Databases*: *Concepts*, *Systems and Applications*, *Proceedings of* 12*th International Conference on Database Systems for Advanced Applications*, *DASFAA* 2007, Bangkok, Thailand, 9-12 April 2007. https://doi.org/10.1007/978-3-540-71703-4_37

[4] Chen, B.-C., Kifer, D., LeFevre, K. and Machanavajjhala, A. (2009) Privacy-Preserving Data Publishing. *Foundations and Trends in Databases*, **2**, 1-167. https://doi.org/10.1561/1900000008

[5] 李杨, 温雯, 谢光强. 差分隐私保护研究综述[J]. 计算机应用研究, 2012, 29(9): 3201-3205.

[6] Sankar, L., Rajagopalan, S.R. and Poor, H.V. (2013) Utility-Privacy Tradeoffs in Databases: An Information-Theoretic Approach. *IEEE Transactions on Information Forensics and Security*, **8**, 838-852. https://doi.org/10.1109/TIFS.2013.2253320

[7] Wagner, I. and Eckhoff, D. (2015) Technical Privacy Metrics: A Systematic Survey. arXiv preprint arXiv:1512.00327

[8] 彭长根, 丁红发, 朱义杰, 等. 隐私保护的信息熵模型及其度量方法[J]. 软件学报, 2016, 27(8): 1891-1903.

[9] Bhamidipati, S., Fawaz, N., Kveton, B. and Zhang, A. (2015) PriView: Personalized Media Consumption Meets Privacy against Inference Attacks. *IEEE Software*, **32**, 53-59. https://doi.org/10.1109/MS.2015.100

[10] Yang, D.Q., Qu, B.Q. and Philippe, C.M. (2019) Privacy-Preserving Social Media Data Publishing for Personalized

Ranking-Based Recommendation. *IEEE Transactions on Knowledge and Data Engineering*, **31**, 507-520. https://doi.org/10.1109/TKDE.2018.2840974

[11] 何凌云，洪良怡，周洁，陈湃卓，赵序琦，谢宇明，刘功申．社交网络隐私安全研究综述[J]．信息技术，2018(5): 153-159.

[12] du Pin Calmon, F. and Fawaz, N. (2012) Privacy against Statistical Inference. https://doi.org/10.1109/Allerton.2012.6483382

[13] Guignard, D. (2019) Partial Differential Equations with Random Input Data: A Perturbation Approach. *Archives of Computational Methods in Engineering*, **26**, 1313-1377. https://doi.org/10.1007/s11831-018-9275-2

[14] Fan, W., He, J., Guo, M., Li, P., Han, Z. and Wang, R.C. (2020) Privacy Preserving Classification on Local Differential Privacy in Data Centers. *Journal of Parallel and Distributed Computing*, **135**, 70-82.