基于奇异值分解的大型社交网络差分隐私算法

郑 剑,杨立聪
(江西理工大学 信息工程学院,江西 赣州 341000)

摘 要:针对基于随机投影的差分隐私算法中存在直接对降维数据直接添加噪声导致基于欧氏距离数据挖掘中数据可用性较差的问题,提出了一种基于奇异值分解的差分隐私算法。该算法首先对高维社交网络的数据利用随机投影进行降维,然后对降维后的数据进行奇异值分解并对奇异值加入高斯噪声,最后通过奇异值分解逆运算生成待发布矩阵。该算法利用的奇异值矩阵是一个仅有主对角线上有值的矩阵,值的个数为矩阵的秩,与直接对降维后的数据直接添加高斯噪声相比,对奇异值矩阵中的值添加高斯噪声能有效地降低噪声的加入量。理论证明该算法满足差分隐私,并设计了欧氏距离差实验和谱聚类实验用于分析算法的数据可用性,实验结果表明该算法的数据可用性高于基于奇异值分解的差分隐私算法。

关键词:社交网络;隐私保护;奇异值分解;随机投影;差分隐私;数据发布
中图分类号:TP309.2 **文献标识码**:A **文章编号**:1673-629X(2022)03-0126-06
doi:10.3969/j.issn.1673-629X.2022.03.021

Differential Privacy Algorithm for Large Social Networks Based on Singular Value Decomposition

ZHENG Jian, YANG Li-cong
(School of Information Engineering, Jiangxi University of Science & Technology, Ganzhou 341000, China)

Abstract: Aiming at the problem of the poor data availability in data mining based on Euclidean distance due to the direct addition of noise to the dimensionality reduction data in the differential privacy algorithm based on random projection, a differential privacy algorithm based on singular value decomposition is proposed. The algorithm firstly uses random projections to reduce the dimensions of high-dimensional social network data, then performs singular value decomposition on the reduced data and adds Gaussian noise to the singular values. Finally, the matrix to be published is generated through the inverse operation of singular value decomposition. The singular value matrix that the proposed algorithm uses is a matrix with values only on the main diagonal, and the number of values is the rank of the matrix. Compared with directly adding Gaussian noise to the data after dimensionality reduction, adding Gaussian noise to singular value matrix can effectively reduce the amount of noise. The theory proves that the proposed algorithm satisfies differential privacy, and the Euclidean distance difference experiment and spectral clustering experiment are designed to analyze the data availability of the algorithm. The experimental results show that the data availability of the proposed algorithm is higher than that of the differential privacy algorithm based on singular value decomposition.

Key words: social network; privacy protection; singular value decomposition; random projection; differential privacy; data release

0 引 言

目前运用于社交网络的差分隐私保护方法主要是关于小型社交网络。尽管这些隐私保护方法可以抵御背景知识攻击来达到保护社交网络的目的,但是随着大数据时代的降临,用户量增大、用户属性增多,这些方法都需要加入大量噪声,导致数据可用性变差。当某网络拥有 n 个社交用户时,需发布 $n \times n$ 的大型矩阵,导致计算和存储成本过高,因此如何提高大型社交网络发布数据的数据可用性显得尤为重要。针对这一思路,该文提出了一种基于奇异值分解的大型社交网络差分隐私保护算法(random projection-singular value decomposition and differential privacy, RP-SVD-DP),RP-SVD-DP 算法利用随机投影将高维社交网络数据映射到低维空间,再对降维后的矩阵进行奇异值分解,

收稿日期:2021-04-13 **修回日期**:2021-08-17
基金项目:国家自然科学基金资助项目(61462034);江西省教育厅科学技术研究项目(GJJ170517)
作者简介:郑 剑(1977-),男,博士,副教授,研究方向为基于隐私保护的数据发布、推荐系统;杨立聪(1996-),男,硕士研究生,研究方向为社交网络与差分隐私。

在奇异值中加入少量差分隐私噪声保护用户隐私,提高发布数据在基于欧氏距离数据挖掘中的数据可用性。

1　相关工作

该文利用差分隐私对社交网络实现隐私保护,因此相关的已有工作包括:黄海平等[1]提出了一种基于非交互的差分隐私保护模型实现对边权的保护。周艺华等[2]提出了基于聚类的社交网络隐私保护方法。朱勇华等[3]提出一种差分隐私保护模型的扰动策略。王丹等[4]提出一种权重社交网络隐私保护算法。刘爽英等[5]提出一种满足差分隐私保护模型的边权重保护策略。Wang Dan 等[6]通过对原始的加权社交网络进行分割,然后在每个子网络利用差分隐私算法来减少噪声的加入量。Li Xiaoye 等[7]提出了一种两步差分私有方法来释放群体间聚类系数的分布。Liu Peng 等[8]提出了一个保留社区结构信息的局部差异隐私模型。但是将这些方法运用到社交网络,需要很高的计算和储存空间,且当用户量大时需要添加大量噪声,影响数据可用性。

随着大数据时代来临,社交网络用户数量庞大且属性值多,兰丽辉等[9]通过重构分割后的社交网络子图并用向量集来表示,构建满足 Johnson-Lindestrauss 定理的映射函数,利用随机投影技术对高维向量集进行降维得到待发布向量集。王婷婷等[10]提出一种基于随机投影的社交网络隐私保护。综上所述,如何能够针对大型社交网络进行隐私保护的算法还相对较少,对高维复杂的社交网络数据进行降维并实现隐私保护,同时保证数据的高可用性,仍然具有挑战性。

针对王婷婷等[10]提出的隐私保护算法中存在对降维数据直接添加噪声导致基于欧氏距离数据挖掘中数据可用性较差的问题,结合随机投影、奇异值分解和差分隐私,提出一种基于奇异值分解的大型社交网络差分隐私保护算法。RP-SVD-DP 算法第一步利用随机投影对高维社交网络图的数据进行降维,第二步对降维后的数据进行奇异值分解并对奇异值加入高斯噪声,最后通过奇异值分解逆运算生成待发布矩阵。利用奇异值矩阵是一个仅有主对角线上有值的矩阵,值的个数为矩阵的秩,与对降维后的数据直接添加高斯噪声相比,对奇异值矩阵中的值添加高斯噪声能有效地降低噪声的加入量。设计基于欧氏距离差实验和基于谱聚类实验对 RP-SVD-DP 算法和基于随机投影社交网络差分隐私算法的数据可用性进行对比分析。

2　相关知识

本章主要介绍差分隐私、社交网络图、随机投影、奇异值分解和 RP-DP 算法的基本概念及相关知识。

2.1　差分隐私

差分隐私[11]是 Dwork 等在 2006 年针对数据库数据隐私保护的问题提出的一种新型隐私保护模型,该模型将随机噪声注入到真实数据集中进行扰乱,达到隐私保护的效果,且数据的整体属性保持不变,扰乱后的数据仍可用于数据挖掘等操作。

定义 1 (ε,δ) - 差分隐私[12]:给定一个随机查询算法 K,对于任意邻近数据集 D 和 D',若 K 在数据集 D 和 D' 查询下得到的结果满足式(1),则称随机查询算法 K 满足 (ε,δ) - 差分隐私。

$$\Pr[K(D)\in S]\leqslant e^{\varepsilon}\times\Pr[K(D')\in S]+\delta \quad (1)$$

其中,$\Pr[\cdot]$ 表示若应用随机查询算法 M 数据可能被泄露的风险;ε 表示随机查询算法 K 所能够提供的隐私保护水平;δ 表示允许每个目标数据都会存在 δ 大小的概率隐私会泄露,δ 的取值通常是很小的常数。

定义 2 高斯机制[12]:对于给定数据集 D,有查询函数 $f:D\rightarrow R^d$,如果有 $c^2>2\ln(1.25/\delta)$,$\sigma\geqslant\Delta_2(f)/\varepsilon$,并且 $N(0,\sigma^2)$ 独立同分布,则算法 A 满足 (ε,δ) 差分隐私。

$$A(D)=f(D)+N(0,\sigma^2) \quad (2)$$

定义 3 敏感度[12]:数据集 D 和 D' 至多相差一条数据集,假设 $\Delta_2(f)$ 是随机查询函数 f 的敏感度,则:

$$\Delta_2(f)=\max_{D,D'}\|f(D)-f(D')\|_2 \quad (3)$$

2.2　社交网络图

社交网络包括用户以及用户之间的关系,通常用图来表示,图 1 是一个简单的社交网络图。其中顶点表示用户,边表示图中两个用户之间的关系。

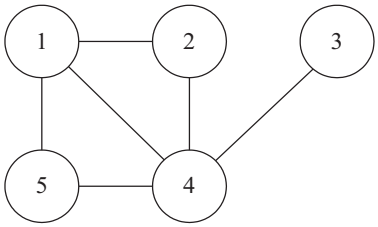

图 1　社交网络图 G

对社交网络图 $G=(V,E)$ 进行差分隐私保护可以转化成对图的邻接矩阵 $\boldsymbol{A}\in\{0,1\}^{n\times n}$ 进行差分隐私保护。其中节点 i 和节点 j 若存在关系则 $A_{ij}=1$,否则 $A_{ij}=0$。图 1 社交网络图对应的邻接矩阵为:

$$\begin{bmatrix}0&1&0&1&0\\1&0&0&0&0\\0&0&0&1&0\\1&0&1&0&1\\1&0&0&1&0\end{bmatrix}$$

2.3　随机投影

随机投影是一种比较有效的降维方法,具有无需考虑原始数据本身固有结构、计算负载低、运行效率高

等特点。随机投影的理论依据是 Johnson-Lindestrauss 定理[13]。

定义 4 Johnson-Lindestrauss 定理(简称 J-L 定理):对给定的失真率 $\varepsilon(0<\varepsilon<1)$ 和任意正整数 d,令整数 $k=O(\log(n)/\varepsilon^2)$,那么对于任意 R^d 空间中的 n 个点构成的集合 V,始终存在一个映射 $f:R^d\rightarrow R^k$ 使得所有的 $x,y\in V$,有:

$$(1-\varepsilon)\|x-y\|_2^2\Delta\leqslant\|f(x)-f(y)\|_2^2\leqslant(1+\varepsilon)\|x-y\|_2^2 \tag{4}$$

2.4 奇异值分解

奇异值分解(singular value decomposition,SVD)属于线性代数中的一种矩阵分解,广泛应用于机器学习的领域中。

定义 5 奇异值分解[14]:设 $m\times n$ 阶矩阵 $\boldsymbol{A}$,且 $m\geqslant n\geqslant 0$。令 $\boldsymbol{A}$ 的秩为 r,则存在酉矩阵 $\boldsymbol{U}$、$\boldsymbol{V}$ 使得:

$$\boldsymbol{A}=\boldsymbol{U}\begin{pmatrix}\boldsymbol{\Sigma} & 0\\ 0 & 0\end{pmatrix}\boldsymbol{V}^{\mathrm{T}} \tag{5}$$

其中,$\boldsymbol{\Sigma}=\mathrm{diag}[\upsilon_1,\upsilon_2,\cdots,\upsilon_r]$ 为对角矩阵,$|\boldsymbol{\Sigma}|=r$,υ_i 为 $\boldsymbol{A}$ 的奇异值,且 $\upsilon_1\geqslant\upsilon_2\geqslant\cdots\geqslant\upsilon_r\geqslant 0$,$\boldsymbol{U}$、$\boldsymbol{V}$ 分别为 $\boldsymbol{A}$ 的左右奇异向量。

定义 6 Mirsky 定理[15]:令 $\boldsymbol{X}$ 与 $\boldsymbol{X}'$ 为具有相同奇异值数的两个矩阵,且:

$$\begin{aligned}&\upsilon_1\geqslant\upsilon_2\geqslant\cdots\geqslant\upsilon_p\\&\upsilon_1'\geqslant\upsilon_2'\geqslant\cdots\geqslant\upsilon_p'\end{aligned} \tag{6}$$

那么对于任意的酉不变范数 $\|\cdot\|$,有:

$$\|\mathrm{diag}(\upsilon_i'-\upsilon_i)\|\leqslant\|\boldsymbol{X}'-\boldsymbol{X}\| \tag{7}$$

定义 7 矩阵 2-范数[16]:对于矩阵 $\boldsymbol{A}(m\times n)$,$A_{ij}$ 为 $\boldsymbol{A}$ 中对应位置的元素,则它的 2-范数为:

$$\|\boldsymbol{A}\|_2=\sqrt{\lambda_1} \tag{8}$$

其中,λ_1 为 $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}$ 的最大特征值。

2.5 RP-DP 算法

基于随机投影的社交网络差分隐私算法(random projection and differential privacy,RP-DP)是王婷婷等[10]针对有 n 个用户的社交网络数据,结合随机投影提出的差分隐私算法。该算法通过对原始社交网络图的邻接矩阵利用随机投影进行降维,再对降维矩阵加入高斯噪声,最后发布经过混淆的矩阵。算法的步骤如下:

输入:具有 n 个用户的社交网络 G

输出:待发布矩阵 $\tilde{\boldsymbol{A}}$

(1)生成社交网络图 G 的邻接矩阵 $\boldsymbol{A}$;

(2)生成投影矩阵 $\boldsymbol{P}$;

(3)利用随机投影生成低维矩阵 $\boldsymbol{A}_p=\boldsymbol{A}\times\boldsymbol{P}$;

(4)生成噪声矩阵 $\Delta\sim N(0,\sigma^2)$;

(5)计算待发布矩阵 $\tilde{\boldsymbol{A}}=\boldsymbol{A}_p+\Delta$。

RP-DP 算法利用随机投影将原始社交网络从 $n\times n$ 维高维矩阵 $\boldsymbol{A}$ 转化为 $m\times n$ 低维矩阵 $\boldsymbol{A}_p$,其中 $m\ll n$,简化了算法的计算复杂性。但 RP-DP 算法存在一个问题,在步骤 4 中生成的噪声矩阵 $\Delta\in R^{n\times m}$ 仍是 $m\times n$ 维的,所带来的噪声对数据的可用性破坏仍是十分巨大的。在 RP-DP 算法中,对数据集中任意两个用户 x,y,记两个用户之间的原始距离为 $\mathrm{dist}(x,y)=\|x-y\|_2$。经过 RP-DP 算法输出后可得 $x'=xP+\Delta_1$,$y'=yP+\Delta_2$,则用户之间的欧氏距离为:

$$\mathrm{dist}(x',y')=\|x'-y'\|_2=\|(x-y)P+\Delta_1+\Delta_2\|_2 \tag{9}$$

其中经 RP-DP 算法扰动后用户之间距离平方的期望为:

$$E[\mathrm{dist}^2(x',y')]=\|x-y\|_2^2+2m\sigma^2 \tag{10}$$

根据期望公式可知,原始数据中任意两个用户之间扰动后距离的平方比原始距离的平方的期望值多一个定值 $2m\sigma^2$。因此减少加入噪声矩阵的维度 m 可以减少加入的噪声量,使扰动后的期望值更低。因此引入奇异值分解,对投影后的矩阵进行奇异值分解,对奇异值添加高斯噪声,添加更少的噪声,提高数据可用性。

3 RP-SVD-DP 算法

考虑到 RP-DP 算法中存在将高维数据降低至低维数据中直接添加高斯噪声会产生较大噪声量的问题,该文提出一种基于奇异值分解的社交网络差分隐私算法。

3.1 算法概述

RP-SVD-DP 算法将随机投影、奇异值分解相结合解决了 RP-DP 算法中加入噪声量较大的问题。RP-SVD-DP 算法首先生成社交网络的邻接矩阵,利用随机投影将高维矩阵转化为低维矩阵,然后对低维矩阵进行奇异值分解,分解成左奇异矩阵、右奇异矩阵和奇异值矩阵,最后对奇异值矩阵添加高斯噪声,根据奇异值分解逆运算生成待发布矩阵。

RP-SVD-DP 算法对奇异值矩阵添加噪声,因为奇异值矩阵只有主对角线上有值,并且值的个数为矩阵的秩,相比于 RP-DP 算法中的 $m\times n$ 维的噪声矩阵 Δ,有效地减小了算法对数据集添加的噪声量。

3.2 算法流程

算法的整体目标是:假定攻击者在拥有最大背景知识的情况下,保护社交网络中用户之间的欧氏距离信息不被泄露。给定一个社交网络 G,发布一个满足 (ε,δ)-差分隐私的待发布矩阵 $\hat{\boldsymbol{A}}$,并且尽可能地保留原始社交网络的结构特性,提高发布数据在基于欧

氏距离挖掘的数据可用性。算法流程如图 2 所示。

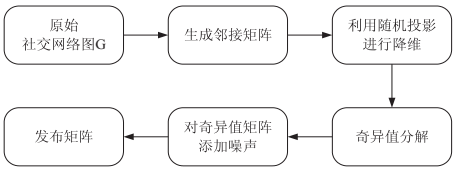

图 2　RP-SVD-DP 算法流程

根据流程图可知,算法大致可以分为 7 个步骤:

(1)对原始社交网络图进行预处理,计算其邻接矩阵 $\boldsymbol{A}$, $\boldsymbol{A} \in R^{n\times n}$;

(2)生成一个随机高斯矩阵 $\boldsymbol{P}$,矩阵 $\boldsymbol{P}$ 中的随机数服从高斯分布 $N(0,1/m)$;

(3)利用随机高斯矩阵 $\boldsymbol{P}$ 计算投影后矩阵 $\boldsymbol{A}_P = \boldsymbol{A} \times \boldsymbol{P}, \boldsymbol{A}_P \in R^{n\times m}$;

(4)对矩阵 $\boldsymbol{A}_P$ 进行奇异值分解 $\boldsymbol{A}_p = U_A^{m\times m} D_A^{m\times n} (V_A^{n\times n})^{\mathrm{T}}$;

(5)对奇异值 υ 添加高斯噪声 $\Delta \sim N(0,\sigma^2)$ 得到 υ' ;

(6)对 υ' 重新排序并去掉小于 0 的奇异值,得到新的奇异值矩阵 $\hat{\boldsymbol{D}}_A^{m\times n}$;

(7)计算 $\hat{\boldsymbol{A}} = \boldsymbol{U}_A^{m\times m} \hat{\boldsymbol{D}}_A^{m\times n} (\boldsymbol{V}_A^{n\times n})^{\mathrm{T}}$,得到待发布矩阵 $\hat{\boldsymbol{A}}$ 。

3.3　算法伪代码

算法 1:RP-SVP-DP 算法。

Input:Original social network Graph G

Output: Release matrix $\hat{\boldsymbol{A}}$

(1) adjacency matrix $\boldsymbol{A} \leftarrow G, A \in R^{n\times n}$

(2) Projection matrix $\boldsymbol{P} \leftarrow \boldsymbol{P}_{i,j} \sim N(0,\frac{1}{m})$

(3) Dimension reduction $\boldsymbol{A}_p = \boldsymbol{A} \times \boldsymbol{P}$

(4) singular value decomposition $\boldsymbol{A}_p = \boldsymbol{U}_A^{m\times m} \boldsymbol{D}_A^{m\times n} (\boldsymbol{V}_A^{n\times n})^{\mathrm{T}}$

(5) Add noise $\Sigma' = \Sigma + \Delta \sim N(0,\sigma^2)$

(6) Reorder matrix $\hat{\boldsymbol{D}}_A^{m\times n}$

(7) Generating matrix $\hat{\boldsymbol{A}} = \boldsymbol{U}_A^{m\times m} \hat{\boldsymbol{D}}_A^{m\times n} (\boldsymbol{V}_A^{n\times n})^{\mathrm{T}}$

原始社交网络图 G 要转换成 RP-SVD-DP 算法处理后的待发布矩阵 $\hat{\boldsymbol{A}}$ 需要经历以下几个步骤:第一步生成图 G 的邻接矩阵 $\boldsymbol{A}$,如算法第 1 行所示;第二步对利用随机投影对邻接矩阵 $\boldsymbol{A}$ 进行指定维数 m 降维,如算法第 2 ~ 3 行所示;第三步对降维后的矩阵 $\boldsymbol{A}_p$ 进行奇异值分解,如算法第 4 行所示;第四步对奇异值矩阵中加入高斯噪声,并返回排序后的奇异值矩阵,如算法第 5 ~ 6 行所示;第五步通过奇异值分解逆运算生成待发布矩阵 $\hat{\boldsymbol{A}}$,如算法第 7 行所示。

3.4　算法隐私性分析

首先计算经随机投影降到 m 维后的矩阵多维奇异值查询函数的全局敏感度。令查询函数 $f: D \rightarrow R^d$,输入为图 G(含 n 的节点),整数 $m(1 \leqslant m \leqslant n)$,输出为图 G 经随机投影降维后矩阵的奇异值组成的向量。

不失一般性,在原图 G 中对节点 v 与 u 之间的边权重改变 1,作为 D' 。令图 G 的邻接矩阵为 $\boldsymbol{A}$,则有 $\| \boldsymbol{A} - \boldsymbol{A}' \|_2 = 1$。令经过随机投影降维后的矩阵为 $\boldsymbol{A}_p$,则有:

$$\| \boldsymbol{A}_p - \boldsymbol{A}_p' \|_F = \| (\boldsymbol{A} - \boldsymbol{A}')\boldsymbol{P} \| \leqslant \max_{1\leqslant i\leqslant m} \sqrt{\sum_{j=1}^{m} (\boldsymbol{P}_{i,j})^2} = 1 \tag{11}$$

其中, $\boldsymbol{P}_{i,j}$ 是服从 $N(0,1/m)$ 的正态分布。

令 υ_i 为图 G 的第 i 个奇异值, υ_i' 为图 G' 的第 i 个奇异值, k 为矩阵奇异值数量,则对于查询函数 $f(G, m, k)$,根据定义 3 可知,它的敏感度为:

$$\Delta_2(f) = \max_{G,G',s.t.\ G'\in\Gamma(G)} \| f(G,m,k) - f(G',m,k) \|_2 = \| (\upsilon_1 - \upsilon_1', \upsilon_2 - \upsilon_2', \cdots, \upsilon_k - \upsilon_k') \|_2 = \sqrt{\sum_{j=1}^{k} (\upsilon_i - \upsilon_i^2)} \leqslant \| \mathrm{diag}(\upsilon_1 - \upsilon_1', \upsilon_2 - \upsilon_2', \cdots, \upsilon_N - \upsilon_N') \|_F$$

由定义 7 可知:

$$\Delta_2(f) \leqslant \| \boldsymbol{A}_p - \boldsymbol{A}_p' \|_F = 1 \tag{12}$$

所以根据高斯机制定义 2,当 $c^2 > 2\ln(1.25/\delta)$, $\sigma \geqslant c\Delta_2(f)/\varepsilon$,即 $\sigma \geqslant \sqrt{2\ln(1.25/\delta)}/\varepsilon$ 并且 $N(0, \sigma^2)$ 独立同分布时,其中 $\Delta_2(f) = 1$,RP-SVD-DP 算法满足 (ε,δ) 差分隐私算法。

3.5　数据可用性保障

本节分析原始数据经过 RP-SVD-DP 算法保护后,任意两个用户之间的欧几里得距离的平方在期望值相对不变,即保证原始社交网络数据在基于欧氏距离分析挖掘中的数据可用性。

对数据中任意两个用户 x, y ,记两个用户之间的原始距离为 $\mathrm{dist}(x,y) = \| x - y \|_2$。经 RP-SVD-DP 算法输出后,则有 $\mathrm{dist}(x',y') = \| x' - y' \|_2 \| (x-y)P + \Delta_1 + \Delta_2 \|_2$。

令 $\Delta = \Delta_1 + \Delta_2$,因为 $\Delta_1, \Delta_2 \sim N(0,\sigma^2)$,所以 $\Delta \sim N(0,2\sigma^2)$ 。则有:

$$E[\mathrm{dist}^2(x',y')] = E[\| (x-y)P \|_2^2 + 2 < (x-y)P, \Delta > + \| \Delta \|_2^2]$$

记 $t = (x-y)P \in R^m$, $s = (x-y) \in R^n$, $z_1 = \| (x-y)P \|_2^2$, $z_2 = 2 < (x-y)P, \Delta > 0$, $z_3 = \| \Delta \|_2^2$。

$$E(z_1) = E(\sum_{i=1}^{m} t_i^2) = \sum_{i=1}^{m} E(t_i^2) = \sum_{i=1}^{m} E(\sum_{j=1}^{n} P_{i,j,S_j}) = \sum_{i=1}^{m} \frac{1}{m} \sum_{i=1}^{n} S_j^2 = \| x - y \|_2^2$$

易证 $E(z_2)=0$,又因为 $\Delta \sim N(0,2\sigma^2)$,所以 $\|\Delta\|_2^2=\Delta_1^2+\Delta_2^2+\cdots+\Delta_k^2 \sim 2\sigma^2\chi_k^2$,则有 $E(z_3)=2k\sigma^2$。

综上所述:

$$E[\mathrm{dist}^2(x',y')]=E(z_1)+E(z_2)+E(z_3)=\|x-y\|_2^2+2k\sigma^2$$

由 $E[\mathrm{dist}^2(x',y')]=\|x-y\|_2^2+2k\sigma^2$ 对比 RP-DP 算法中的期望 $E'[\mathrm{dist}^2(x',y')]=\|x-y\|_2^2+2m\sigma'^2$,其中 k 为加入高斯噪声后奇异值矩阵的奇异值个数,m 为降维的维数。根据定义 7 中 $\left|\sum\right|=r$,r 为矩阵 $\boldsymbol{A}_p$ 的秩,其中 $r\leqslant m$ 且 $\upsilon_i>0$。由于加入高斯噪声会使得原奇异值矩阵中的奇异值出现小于 0 的情况,故 $k<r\leqslant m$,即 $k<m$。在 RP-DP 算法中 $\sigma=\sqrt{2\ln(2/\delta)+\varepsilon}/\varepsilon$,在 RP-SVD-DP 算法中 $\sigma'=\sqrt{2\ln(1.25/\delta)}/\varepsilon$,在相同 ε,δ 下,$\sigma'<\sigma$,故 RP-SVD-DP 算法的数据效用性高于 RP-RP 算法。

4 实验设计与结果分析

4.1 实验环境与实验设计

硬件环境:Intel(R) Xeon(R) CPU E5-2680 v3 @ 2.50 GHz;32 G 内存;1 T 硬盘。

软件环境:Windows 10,64 位操作系统;Python3。

实验数据采用了斯坦福大学公开数据集 SNAP Social network 中的 Bitcoin OTC 子集(含 5 881 个节点 35 592 条边)。

为了对 RP-SVD-DP 算法和 RP-DP 算法基于欧氏距离数据挖掘中的数据可用性进行对比分析,本节设计了两个实验。第一个实验为基于欧氏距离差的实验,通过计算经过 RP-SVD-DP 算法和 RP-DP 算法隐私保护后的待发布矩阵中用户间欧氏距离和原始社交网络图中用户之间的欧氏距离之差来衡量算法的数据可用性;第二个实验为基于谱聚类的实验,对经过 RP-SVD-DP 算法和 RP-DP 算法隐私保护后的待发布矩阵进行谱聚类,通过计算标准化互信息 NMI 来衡量算法的数据可用性。

4.2 欧氏距离差实验

为了对所提出的 RP-SVD-DP 算法和 RP-DP 算法添加的噪声量做统一的度量,用待发布矩阵用户间的欧氏距离和原始社交网络图中用户之间的欧氏距离之差来衡量算法的数据可用性,以此为评价依据衡量噪声加入量所带来数据可用性的变化。实验从 Bitcoin OTC 数据集中随机采样选取了 600 名用户(约为总体十分之一),并计算用户原始欧氏距离分别经 RP-DP 算法和 RP-SVD-DP 算法在相同隐私保护水平下扰动后的用户间欧氏距离差。在实验中,将原始数据集降至 500 维,即 $m=500$,以及差分隐私保护水平分别设为 $\varepsilon=0.3,0.5.0.7.0.9$,为了提高实验结果的准确性,在每个隐私预算下进行十次实验取平均值。实验结果如表 1 所示。

表 1 不同隐私保护算法用户间欧氏距离差

ε	RP-DP	RP-SVD-DP
0.3	8.596	2.161
0.5	4.865	1.852
0.7	3.373	1.668
0.9	2.252	1.246

分析表 1 数据可知,RP-DP 算法和 RP-SVD-DP 算法的欧氏距离差不大,说明算法都满足 J-L 定理,且欧氏距离差随着隐私预算 ε 的变大而变小。在相同的隐私预算 ε 下,RP-SVD-DP 算法的用户间欧氏距离差均小于 RP-DP 算法,且随着隐私预算不断减小,RP-SVD-DP 算法欧氏距离差的增长幅度也小于 RP-DP 算法,说明 RP-SVD-DP 算法的数据可用性优于 RP-DP 算法。由实验结果得出,RP-SVD-DP 算法加入的噪声量低于 RP-DP 算法。

4.3 谱聚类实验

为了对所提出的 RP-SVD-DP 算法和 RP-DP 算法发布的数据在基于欧氏距离数据挖掘中数据可用性做统一的度量,用标准化互信息 NMI 衡量算法的数据可用性,以此为评价依据衡量投影数量 m 和隐私预算参数 ε 所带来数据可用性的变化。

谱聚类实验分为两部分,分别改变随机投影数量 m 和差分隐私保护水平 ε,对原始数据集进行聚类,通过计算不同隐私保护算法下的标准化互信息 NMI 来衡量发布数据集的数据可用性程度。

在改变随机投影数量 m 的对比实验中,将算法的差分隐私保护水平分别设为 $\varepsilon=0.5$ 和 $\varepsilon=0.9$。通过将原始数据集从高维数据转化为不同维数的低维数据,对比两算法 NMI 值的大小,从而分析算法数据可用性,实验结果如表 2 所示。

表 2 不同随机投影数量 m 值,算法发布数据集谱聚类的 NMI 值对比

m	RP-DP		RP-SVD-DP	
	$\varepsilon=0.5$	$\varepsilon=0.9$	$\varepsilon=0.5$	$\varepsilon=0.9$
100	0.315	0.467	0.423	0.472
300	0.407	0.516	0.469	0.621
500	0.491	0.617	0.578	0.877
700	0.537	0.651	0.647	0.905
900	0.571	0.677	0.681	0.947

分析表 2 可知,RP-SVD-DP 算法和 RP-DP 算法的 NMI 值均随着随机投影数量 m 的增大而增大,说明

将原始高维数据的维度降的越低,所丢失掉的信息越多,导致算法的数据可用性越差。在相同差分隐私保护水平的情况下,RP-SVD-DP 算法的 NMI 值均高于 RP-DP 算法。当 $m=500$, $\varepsilon=0.9$ 时,RP-SVD-DP 算法的 NMI 值达到了 0.947,而 RP-DP 算法的 NMI 值只有 0.677;当 $m=500$, $\varepsilon=0.5$ 时,RP-SVD-DP 算法和 RP-DP 算法的 NMI 值分别为 0.578 和 0.491。由实验结果得出,在相同的隐私预算下,将原始数据集降低至不同维度,RP-SVD-DP 的数据可用性均优于 RP-DP 算法。

在改变差分隐私保护水平 ε 的对比实验中,将原始数据集通过随机投影降低至 500 维,即 $m=500$,将差分隐私保护水平 ε 设为不同值,对比两算法的 NMI 值大小,分析算法数据可用性,实验结果如表 3 所示。

表 3　不同隐私保护算法发布数据集相对原始数据集谱聚类的 NMI 对比($m=500$)

ε	RP-DP	RP-SVD-DP
0.1	0.325	0.446
0.3	0.357	0.513
0.5	0.492	0.577
0.7	0.536	0.748
0.9	0.675	0.943

分析表 3 可知,在相同的投影维度 $m=500$ 的情况下,RP-SVD-DP 算法和 RP-DP 算法的 NMI 值均随着隐私保护水平 ε 的增大而增大。由图中曲线可知,当隐私保护水平 $\varepsilon=0.3$ 时,RP-SVD-DP 算法的 NMI 值为 0.513,而 RP-DP 算法的 NMI 值仅有 0.357;当隐私保护水平 $\varepsilon=0.7$ 时,RP-SVD-DP 算法的 NMI 值大于 0.748,而 RP-DP 算法的 NMI 值仅有 0.536。由实验结果得出,把原始数据集降低至相同维度,在不同的隐私预算下 RP-SVD-DP 的数据可用性均优于 RP-DP 算法。

5　结束语

为解决 RP-DP 算法中因噪声过大导致数据可用性低的问题,提出了一种改进的 RP-SVD-DP 算法。在 RP-SVD-DP 算法中,先对原始数据利用随机投影进行降维;再对降维后的数据进行奇异值分解,对奇异值矩阵加入差分隐私噪声;最后发布加噪后的数据。实验表明,RP-SVD-DP 算法在基于欧氏距离的实验中加入的噪声量更少,数据可用性优于 RP-DP 算法。提出的基于奇异值分解的社交网络差分隐私算法是一种非交互式隐私保护方法,无法做到数据的实时更新发布,在大数据时代,数据通常都是实时变化的,所以下一步要将该算法扩展至交互式,尽可能地保证数据的实时性。

参考文献:

[1] 黄海平,张东军,王　凯,等. 带权值的大规模社交网络数据隐私保护方法[J]. 计算机研究与发展,2020,57(2):363-377.

[2] 周艺华,张　冰,杨宇光,等. 基于聚类的社交网络隐私保护方法[J]. 计算机科学,2019,46(10):154-160.

[3] 朱勇华,刘爽英. 加权社交网络敏感边的差分隐私保护研究[J]. 计算机应用研究,2018,35(11):3436-3440.

[4] 王　丹,龙士工. 权重社交网络隐私保护中的差分隐私算法[J]. 计算机工程,2019,45(4):114-118.

[5] 刘爽英,朱勇华. 针对社交网络边权重的差分隐私保护[J]. 计算机工程与设计,2018,39(1):44-48.

[6] WANG Dan, LONG Shigong. Boosting the accuracy of differentially private in weighted social networks[J]. Multimedia Tools and Applications,2019,78(24):34801-34817.

[7] LI Xiaoye, YANG Jing, SUN Zhenlong, et al. Differentially private release of the distribution of clustering coefficients across communities[J]. Security and Communication Networks,2019,2019:1-9.

[8] LIU Peng, XU Yuanxin, JIANG Quan, et al. Local differential privacy for social network publishing[J]. Neurocomputing,2020,391:273-279.

[9] 兰丽辉,鞠时光. 一种基于随机投影的加权社会网络隐私保护方法[J]. 计算机科学,2016,43(3):151-157.

[10] 王婷婷,龙士工,丁红发. 大型社交网络的差分隐私保护算法[J]. 计算机工程与设计,2020,41(6):1568-1574.

[11] DWORK C. Differential privacy[C]//Automata, languages and programming. Venice, Italy: Springer,2006:1-12.

[12] LIU F. Generalized Gaussian mechanism for differential privacy[J]. IEEE Transactions on Knowledge and Data Engineering,2018,31(4):747-756.

[13] DIRKSEN S. Dimensionality reduction with subgaussian matrices: a unified theory[J]. Foundations of Computational Mathematics,2016,16(5):1367-1396.

[14] CHUNG F R K, GRAHAM F C. Spectral graph theory[M]. American: American Mathematical Soc. ,1997.

[15] STEWART G W. Matrix perturbation theory[M]. [s. l.]: Academic Press,1990:1-32.

[16] 戴　华. 矩阵论[M]. 北京:科学出版社,2001.