

基于加性噪声的强鲁棒数据库盲水印方法

李 程, 张国栋

(中国人民解放军 96713 部队, 江西 上饶 334000)

摘 要: 针对大数据共享和发布过程中面临的侵权盗版与隐私泄露问题, 提出了一种基于加性噪声的强鲁棒数据库盲水印方法。该方法结合了数据库水印与数据脱敏技术, 利用加性拉普拉斯噪声已有失真, 通过比值奇偶性与噪声修改机制嵌入水印信息, 显著减少二次失真, 并通过统计特征调整, 保持数据的可用性。该方法在强化隐私保护性能的同时, 实现水印信息盲提取, 并具备极强的鲁棒性。实验证明, 该方法有效降低了数据泄露和被盗用的风险, 是一种同时实现敏感数据的隐私保护、泄密溯源与版权标识的集成式方案。

关键词: 数据库水印; 数据脱敏; 数据安全; 隐私保护

中图分类号: TP309.2

文献标识码: A

DOI: 10.19358/j.issn.2097-1788.2025.02.005

引用格式: 李程, 张国栋. 基于加性噪声的强鲁棒数据库盲水印方法 [J]. 网络安全与数据治理, 2025, 44(2): 32 - 38, 43.

A robust blind watermarking method for databases based on additive noise

Li Cheng, Zhang Guodong

(Unit 96713 of the People's Liberation Army, Shangrao 334000, China)

Abstract: A robust blind watermarking method for databases based on additive noise is proposed to address the issues of copyright infringement and privacy breaches in the process of big data sharing and publishing. This method integrates database watermarking with data desensitization techniques, leveraging the inherent distortion of additive Laplace noise. Watermark information is embedded through the ratio parity and noise modification mechanisms, significantly reducing secondary distortion. By adjusting statistical characteristics, the method preserves data usability. While enhancing privacy protection, it enables blind extraction of watermark information and demonstrates exceptional robustness. Experimental results show that this approach effectively reduces the risks of data leakage and unauthorized use, providing an integrated solution that simultaneously achieves sensitive data privacy protection, leakage tracing, and copyright marking.

Key words: database watermarking; data desensitization; data security; privacy protection

0 引言

随着大数据时代的全面来临和信息技术的迅速发展, 数据在现代社会中扮演着愈发重要的角色, 其中大量的个人数据被收集、存储和共享, 这些个人数据通常存储在数据库中并具有非常高的使用价值, 数据拥有者可以通过大数据分析帮助企业了解用户的喜好、行为和需求, 实现个性化推荐、定制化服务和有效决策^[1-2]。但数据库在使用过程中面临着数据盗窃、非法复制和侵犯版权等问

认为关键问题之一^[5]。

如何在不影响数据使用便利性的前提下, 加强对数据安全与隐私信息的保护已成为社会各界共同关注的目标。在此背景下, 数据库水印技术和数据脱敏技术成为解决上述问题的有效手段, 并在数据安全和隐私保护领域得到广泛应用。

1 相关研究

1.1 数据库水印

数据库水印是一种重要的信息隐藏技术, 其核心思想是通过隐秘的方式将有意义的水印信息 (版权说明、用户身份等) 嵌入到数据库中, 在需要时可提取水印, 实现数据库的版权保护、篡改检测、泄密溯源以及完整

性认证等多重目标^[6]。

2002年, Agrawal 等人^[7]首次提出了数据库水印技术, 并用于关系型数据库的保护。之后, 数据库水印技术得到长足的发展。根据应用场景的不同, 数据库水印技术可分为两种类型: 鲁棒水印^[8-9]和脆弱水印^[10-11]。鲁棒水印是一种能够抵抗各种攻击和变换的数字水印, 通常应用于对版权保护、内容认证、数据完整性验证等具有高要求的场景。脆弱水印是一种对数据进行微小修改后就会发生变化或破坏的数字水印, 主要用于数据的完整性验证和真实性认证。

根据水印载体是否修改, 数据库水印技术可以分为有失真水印方法^[12-13]和无失真水印方法^[14-15]。有失真水印方法考虑水印信息对各种可能攻击的抵抗能力, 但会对原始数据造成永久失真, 降低数据质量和可用性。无失真水印不会修改数据库中的原始数据, 以保持原始数据的完整性和准确性。

1.2 数据脱敏

数据脱敏技术是一种用于保护敏感数据隐私的方法, 通过对数据中的敏感信息进行修改或删除, 以减少通过数据分析识别个人敏感信息的能力, 同时保留数据的有效性和可用性。该技术在数据共享、数据发布、数据分析等场景中起着重要作用。

Adam 等人^[16]最早于1989年提出了数据脱敏的概念。传统数据脱敏方法是保护敏感数据隐私的重要手段, 通过对数据进行不同方式的处理, 实现对敏感信息的隐藏或变换, 从而降低数据泄露的风险。这些方法^[17-20]包括泛化、抑制、排列、扰动、掩码、替换和加密等。每种方法都有其独特的特点和适用场景, 在数据隐私保护和信息安全领域发挥着重要作用。

1.3 数据安全与隐私保护

将数据库水印技术与数据脱敏技术相结合, 可以实现对数据库的全面保护, 有效降低数据泄露和盗用的风险, 使数据库在管理、传输和共享过程中更加安全可靠。

2005年, Bertino 等人^[21]在医疗数据共享中首次注意到版权与隐私信息的双重保护功能, 综合利用分箱 (bin-

ning) 和数字水印技术的统一框架, 实现了对外部数据的全面保护。这种方法本质上只是将两种技术融合到一个框架中, 并不是一种集成式方案。2017年和2021年, Nakamura 等人^[22-23]分别提出了两种用于匿名数据的水印方法, 通过对敏感数据进行替换操作, 使用替换操作的数量来表示水印信息, 但其方法的水印嵌入与提取仍然是非盲的且仅适用于文本型数据。Bordel 等人^[24]提出了一种新的机制来保护、验证和匿名化5G网络支持的物联网 (IoT) 系统中的数据, 使用了数字水印技术和轻量级密码技术, 具有良好的安全性, 但由于混沌动力学的引入, 每分钟的数学运算量较高。2022年, Yu 等人^[25]提出了一种基于k匿名数据集的鲁棒性水印方案, 通过准标识符属性来实现定位功能, 在非敏感属性中嵌入水印信息, 是一种同时实现版权保护与隐私保护的方案, 但该方法的信息损失和计算开销较大。

综上所述, 虽然结合数据库水印与数据脱敏技术的方案思路提出时间很早, 但能同时实现泄密溯源与版权保护、隐私信息保护双重功能的集成方案非常少, 且存在着水印提取非盲、适用数据类型单一、信息损失和计算开销大等缺点。

针对以上问题, 本文提出了一种基于加性噪声的强鲁棒数据库盲水印方法 (Additive Noise Database Watermarking, ANDW), 主要贡献点如下:

(1) 提出一种数据库水印方案, 能同时实现隐私信息保护、版权标识和泄密溯源, 是一种轻量化、易实现的集成式方案;

(2) 制定了水印信息表示策略, 设计了基于加性噪声的水印嵌入算法, 实现水印盲提取, 具有极强的鲁棒性;

(3) 水印嵌入算法利用加性拉普拉斯噪声自身造成的失真嵌入水印信息, 显著减少了嵌入阶段的二次失真, 并利用统计特征调整, 保留了数据的可用性。

2 方法设计

本文提出的基于加性噪声的强鲁棒数据库盲水印方法 (ANDW) 主要包括3个阶段: (1) 数据预处理; (2) 水印嵌入; (3) 水印提取。其方案框架如图1所示。

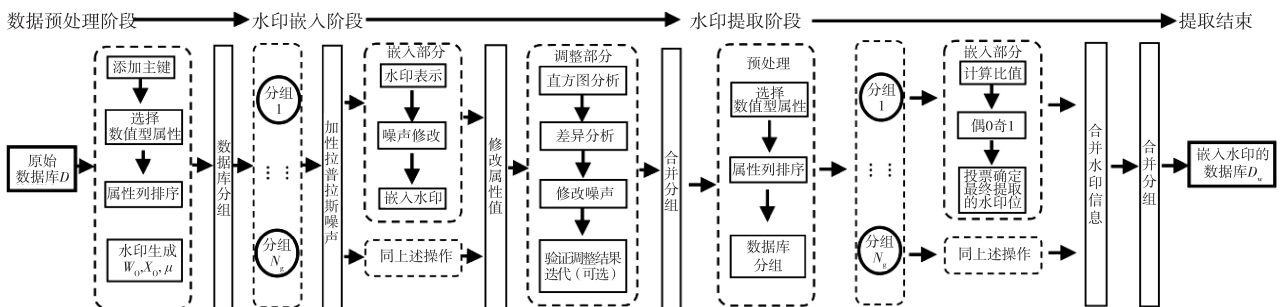


图1 ANDW 方案框架图

2.1 数据预处理阶段

数据预处理阶段主要步骤包括: 选择数值型数据的属性列、通过属性名对属性列进行升序排序或降序排序、对元组添加主键、对数据库元组进行分组、生成水印信息等。

2.1.1 数据库分组

为了使水印信息能够分散地嵌入整个数据库中, ANDW 方法需要通过式 (1) 将数据库分成对应的组数, 每组中包含的元组均不相同。

$$n_i = H(K_s \| H(K_j \| pKey_m)) \% N_g \quad (1)$$

其中, $pKey_m$ 表示第 m 行元组的主键值, K_s 表示分组使用的主密钥, K_j 表示第 j 列属性值分组时使用的密钥, n_i 是第 m 行元组所在的分组编号, $n_i = 0, 1, 2, \dots, N_g$, N_g 为分组数 (水印长度), $H()$ 表示哈希函数, $\|$ 表示连接符号。

通过对不同的属性列使用不同的分组密钥 K_j , 可以增加数据库分组信息的安全性和水印的鲁棒性, 即使攻击者知道了分组主密钥 K_s , 也无法知道每个属性列的分组情况。

2.1.2 水印信息生成

水印信息通常是将一些特定的标识符 (比如用户 ID) 转换成二进制串。ANDW 方法并不是将二进制原始数据嵌入数据库, 而是通过基于一维 Logistic 映射的置乱方法, 将原始水印信息 W_0 的顺序进行置乱处理, 得到置乱后的水印信息 W_s , 再将 W_s 嵌入数据库中。

Logistic 映射是一类非常简单的混沌系统, 在数据安全和保密通信中应用广泛。其数学表达式如下:

$$X_{n+1} = \mu X_n (1 - X_n), \quad n = 0, 1, 2, 3, \dots \quad (2)$$

其中, $\mu \in [0, 4]$, $X_n \in (0, 1)$ 。当 $\mu \in (3.569\ 945, 4]$ 时, Logistic 映射处于混沌状态, 即 $\{X_n\}$ 对初始值非常敏感。因此, 置乱后的水印信息具有很强的随机性, 即使攻击者提取到了数据库中的所有二进制位, 也会因没有初始值 X_0 和 μ 而无法还原得到原始的水印信息串, 从而提高了水印的安全性。

2.2 水印嵌入阶段

水印嵌入阶段框架图如图 1 所示。ADNW 方法首先利用加性拉普拉斯噪声, 对数据库中的数值型敏感属性列进行数据脱敏处理。然后, 将分组中的元组分为嵌入部分和调整部分, 对嵌入部分使用本文提出的基于噪声修改机制的水印嵌入算法以嵌入水印信息。值得注意的是, 在每组中所有嵌入部分属性值均嵌入同样的 1 bit 水印信息, 以便于在提取水印时通过投票原则提高鲁棒性。对每个分组重复上述步骤, 将水印信息嵌入所有分组中。最后, 修改调整部分的数据以实现统计特征调整, 使脱

敏并嵌入水印后的整体数据与原始数据的统计特征相似。

2.2.1 加性拉普拉斯噪声脱敏算法

拉普拉斯噪声是一种基于拉普拉斯分布的随机噪声模型, 通常用于保护数据隐私, 其概率密度函数 (Probability Density Function, PDF) 形式为:

$$f(x | \mu_L, b_L) = \frac{1}{2b_L} \exp\left(-\frac{|x - \mu_L|}{b_L}\right) \quad (3)$$

其中, μ_L 是分布的位置参数, 表示分布的中心位置, b_L 是分布的尺度参数, 用于控制分布的分散程度。

将拉普拉斯噪声加到原始数据中, 产生扰动后的数据, 这样做可以隐藏原始数据的细节, 保护个体隐私。拉普拉斯噪声简单易实现, 计算成本低廉, 适用于多种数据类型和应用场景, 具有较好的随机性和隐私保护效果。为了实现数据脱敏, ANDW 方法分别对每列敏感数据添加加性拉普拉斯噪声, 并通过设置隐私预算 ϵ 控制拉普拉斯分布的尺度, 从而影响了添加的噪声的大小和分布的幅度, ϵ 和 b_L 之间的关系通常是 $\epsilon = 1/b_L$ 。

2.2.2 基于比值奇偶性的水印信息表示策略

给定一个步长参数 $step_size$, 通过计算加噪后的属性值与步长 $step_size$ 的比值 K , 利用 K 的奇偶性来表示水印信息 “0” 或 “1”。例如采用 “偶 0 奇 1” 的水印表示策略, 记水印信息为 w :

$$\begin{cases} K = x_i^n \bmod step_size \\ w = K \bmod 2 \end{cases} \quad (4)$$

其中, x_i^n 表示添加加性拉普拉斯噪声后的属性值。

为了更加直观地展示水印信息表示策略, 本文给出一个示例图, 如图 2 所示, 可以看到, 当 $x_i^n \in [step_size, 2 \times step_size)$ 时, 比值 $K = 1$, 此时代表的水印信息 $w = 1$, 依此类推。

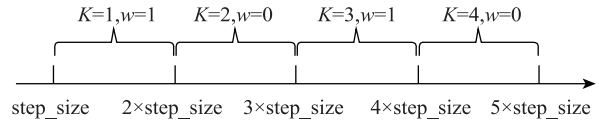


图 2 水印信息表示策略示意图

2.2.3 基于噪声修改机制的水印嵌入算法

在数据库进行分组后, 对于每个分组, 根据式 (5) 将分组内的属性值分为嵌入部分和调整部分。

$$x_i \in \begin{cases} \text{嵌入部分, } H(K_s \| H(K_j \| pKey_i)) \% ea = 0 \\ \text{调整部分, } H(K_s \| H(K_j \| pKey_i)) \% ea \neq 0 \end{cases} \quad (5)$$

其中, $pKey_i$ 是第 i 行元组的主键, ea 是区分嵌入部分和调整部分的参数。

水印嵌入算法的实现过程如下:

(1) 对于添加噪声后的属性值 x_i^n , 如果需要嵌入的水印位 w_i 与 K 的奇偶性一致, 则无需修改噪声值 $noise$ 的大小。

(2) 如果需要嵌入的水印位 w_i 与 K 的奇偶性不一致, 则需要通过修改噪声值 noise , 得到新噪声值 noise' , 使最终的属性值 x'_i 与 step_size 的新比值 K' 与水印位 w_i 的奇偶性一致。为了减小修改噪声过程中所造成的失真, 提高数据的可用性, 新比值 K' 的取值应当为 $K+1$ 或者 $K-1$, 即:

$$K' = (x_i + \text{noise}') \bmod \text{step_size}, K' \in \{K+1, K-1\} \quad (6)$$

具体地, 修改后的噪声值 noise' 计算如下:

$$\text{noise}' = \begin{cases} \text{noise} + \Delta, & \text{if } \text{noise} > 0, \text{ let } K' = K - 1 \\ \text{noise} + \Delta, & \text{if } \text{noise} < 0, \text{ let } K' = K + 1 \\ \text{noise} + \Delta, & \text{if } \text{noise} = 0, \text{ let } K' = K + 1 \text{ or } K - 1 \end{cases} \quad (7)$$

其中, Δ 是在原噪声上添加的拉普拉斯噪声变化量, 其目的是为了使得 K' 满足要求。

(3) 对该分组中嵌入部分的所有属性值, 均重复上述步骤以嵌入相同的水印信息 w_i 。

(4) 对不同属性列的所有分组均重复上述步骤, 以嵌入所有水印信息位 W 。

为了方便理解, 本文给出基于噪声修改机制的水印嵌入算法的示例, 如图3所示。 x_i^n 与 step_size 的比值 $K=2$, 当需要嵌入的水印信息 $w=0$ 时, 不需要对噪声值进行修改, 而当需要嵌入的水印信息 $w=1$ 时, 需要对噪声值进行修改, 使得新属性值 x'_i 与 step_size 的比值 $K'=1$ 或者 3。

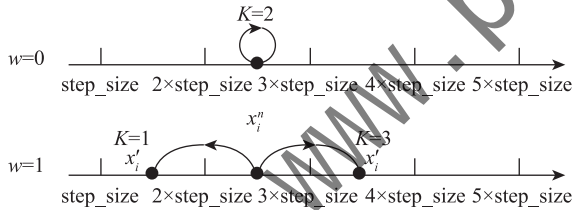


图3 水印嵌入过程示意图

2.2.4 统计特征调整

经过添加加性拉普拉斯噪声和嵌入水印信息后, 与原始数据库相比, 对应列属性值的统计特征可能会发生变化。为了尽可能保持数据的可用性和可分析性, ADNW 方法会对调整部分的属性值进行部分修改, 以实现与原始数据相似的分布特性。具体来说, ADNW 使用直方图匹配法以实现上述功能, 具体步骤如下:

(1) 对原始数据库 D 和水印数据库 D_w 进行直方图分析, 将数据分成若干个区间, 统计每个区间内的数据点数量。

(2) 确定直方图中每个区间的边界。

(3) 对于每个区间, 计算其在 D 和 D_w 中的数据点数

量差异。如果某个区间在 D_w 中的数据点数量较多, 则需要减少该区间的数据点数量; 反之, 如果某个区间在 D_w 中的数据点数量较少, 则需要增加该区间的数据点数量。

(4) 对于每个需要调整区间, 根据其数据点数量差异和调整方向, 进行如下操作:

①如果该区间在 D_w 中的数据点数量较多, 则修改嵌入部分中处于该区间中的一部分数据, 调整至相邻区间, 直到与 D 中相应区间的数据点数量相近。

②如果该区间在 D_w 中的数据点数量较少, 则修改嵌入部分中处于相邻区间内的一部分数据, 调整至该区间, 使得与 D 中相应区间的数据点数量相近。

(5) 调整完成后, 重新计算调整后的 D_w 的直方图, 并与 D 的直方图进行比较, 以验证调整结果是否符合预期。

(6) 如果调整后的 D_w 仍然与 D 存在较大差异, 可以多次迭代调整数据直到满足要求的相似度度量为止。

2.3 水印提取阶段

由于 ADNW 方法属于全盲数据库水印方案, 水印嵌入和提取过程完全独立于原始数据, 通常只依赖于密钥, 在本方法中, 密钥包括水印信息置乱的初始值 X_0 和 μ 、分组的主密钥 K_g 和不同属性列的分组密钥 K_j 。在水印提取阶段, ADNW 方法也无需保存额外的辅助信息 (例如水印嵌入位置、水印嵌入的操作记录等), 仅需要几个参数 (分组数 N_g 、步长 step_size 和分区嵌入与调整部分参数 ea) 即可实现水印的盲提取。

水印提取阶段的框架如图1所示。首先对添加了水印信息的数据库进行与水印嵌入阶段相似的数据预处理。

对于每个数据库分组内的属性值, 具体的水印提取步骤如下:

(1) 根据式 (5) 将属性值分为嵌入部分和调整部分。

(2) 对于每个嵌入部分的属性值, 计算该属性值 x' 与步长 step_size 的比值 K' 。

(3) 通过 K' 的奇偶性来判断该属性值处嵌入的水印信息 “0” 或 “1”。例如采用 “偶0奇1” 的水印表示策略, K' 为偶数表示嵌入的水印信息为 “0”, K' 为奇数表示嵌入的水印信息为 “1”。

(4) 对于每个提取的水印位, 使用投票原则来确定最终水印信息, 例如对于提取的第 i 位水印 w_{ei} , 对于嵌入该位水印的分组中所有嵌入部分的属性值, 均提取对应的水印位, 并统计水印位分别为 0 和 1 的频次, 选择频次较高的水印位作为该分组最终提取出的水印信息 w_{ei} 。

(5) 对于每个数据库分组, 均重复以上步骤, 最终得到提取出的水印信息串 w_e 。

(6) 对水印信息串进行置乱还原, 得到提取出的最终水印信息 W_e 。

3 实验结果与分析

本节实验目的主要是评估 ANDW 的性能, 包括数据失真与隐私保护性能分析、数据可用性测试、水印提取鲁棒性分析和时间复杂度分析等。

实验在一台 3.9 GHz AMD R5 5600G 处理器和 32 GB 内存的计算机上进行。本实验所使用的数据集为加州大学所提供的人口普查数据集 (<http://archive.ics.uci.edu/ml/datasets/adult>), 该数据集根据人口普查数据预测个人年收入是否超过 5 万美元。其总共包含了 32 561 行和 15 列数据。实验中, 选择数据集中的所有数据作为

实验数据, 并且选择 2 个属性列作为敏感属性列 ('age' 和 'hour_per_week')。另外, 对所有元组额外添加一个主键, 因此每个元组总共有 16 个属性。本文中, 数据库分组数 N_g 设置为 48, 步长 $step_size$ 和区分嵌入与调整部分参数 ea 均设置为 5, 拉普拉斯噪声的隐私预算 ϵ 设置为 1。

3.1 数据失真与隐私保护性能分析

本小节实验分析使用 ANDW 对原始数据库进行数据脱敏并添加水印前后, 敏感属性列 'age' 和 'hour_per_week' 的均值 Mean、标准差 Std、平均绝对误差 MAE 以评估 ANDW 方案造成的数据失真, 为了更加直观地展示嵌入水印对数据产生的影响, 同样计算了每个敏感属性列的 Mean 和 Std 的变化, 分别用 DM 和 DS 表示。实验结果如表 1 表示。

表 1 嵌入水印前后数据库不同敏感属性列的均值、标准差及其变化值和 MAE 值

属性名	原始数据库		ANDW		DM	DS	MAE
	Mean	Std	Mean	Std			
age	38.581 65	13.640 43	38.078 62	13.684 73	0.503 03	0.044 30	2.813 25
hour_per_week	40.437 46	12.347 43	40.259 36	12.450 04	0.178 10	0.102 61	

由表 1 可以看出经过 ANDW 方法进行数据脱敏及添加水印后的数据库, 敏感属性列 'age' 和 'hour_per_week' 的 DM 分别为 0.503 03 和 0.178 10, DS 分别为 0.044 30 和 0.102 61, MAE 值也仅为 2.813 25, 均处于非常小的范围, 证明 ANDW 水印方法是高效的、低影响的, 对数据库造成的失真非常小, 不会对数据的整体特征变化造成显著影响。

图 4 和图 5 分别展示了敏感属性列 'age' 和 'hour_per_week' 最终添加的噪声分布情况与拉普拉斯分布的概率密度函数对比结果, 可以看出, 尽管 ANDW 修改了噪声值, 但从实验结果上看, 最终修改的噪声值仍然近似服从拉普拉斯分布, 能够实现良好的数据脱敏效果, 从而同时

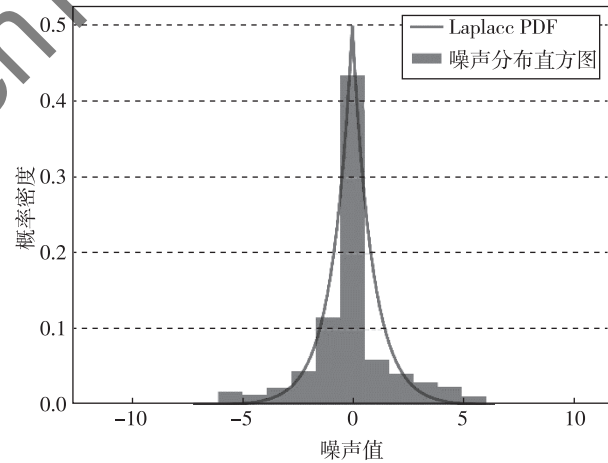


图 5 属性列 'hour_per_week' 的最终噪声分布情况

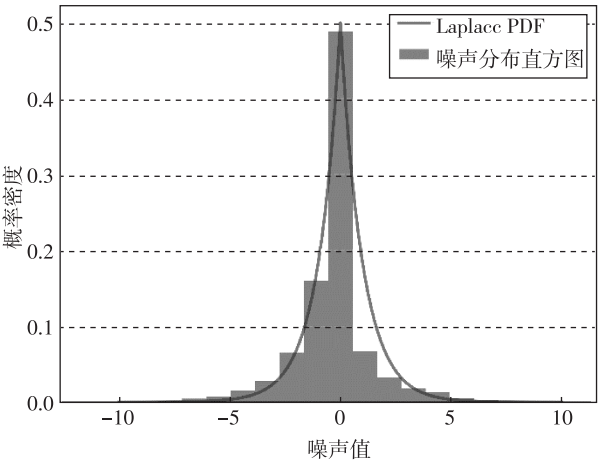


图 4 属性列 'age' 的最终噪声分布情况

实现水印嵌入与数据脱敏功能。

3.2 数据可用性测试

为了评估对使用 ANDW 方法后的数据库进行数据挖掘的可行性, 实验使用随机森林 (Random Forest)、决策树 (Decision Tree)、支持向量机 (SVM) 和 AdaBoost 4 种分类器对森林覆盖类型数据进行分类。分类结果共分两类: 年收入 $\leq 50k$ 和年收入 $> 50k$ 。为了评估这些分类器的性能, 选取数据挖掘分类算法评价中常用的两个指标: 精确度 (Precision, Pre) 和灵敏度 (Sensitivity, Sen)。为了更清楚地表示结果, 本文还计算了水印嵌入前后每个分类的 Pre 和 Sen 的变化量, 分别表示为 DPre 和 DSen。

分类实验结果如表 2 所示, 其中 Pre_o 和 Sen_o 、 Pre_w 和 Sen_w 分别表示嵌入水印前后数据库分类的 Pre 和 Sen 。对于使用 ANDW 进行数据脱敏和嵌入水印后的数据库, 四种分类器中 Random Forest 的分类结果影响最大, 但最大值仅为 2.02%, 其余三种分类器的 $DPre$ 和 $DSen$ 都非常小, 最大仅为 0.69%, 可以证明, ANDW 方法对数据挖掘分类效果的影响非常小, 能够实现与原数据库几乎相同的数据挖掘分类性能。

表 2 不同分类器对嵌入水印前后数据库进行数据挖掘分类的性能对比 (%)

分类器	类别	Pre_o	Pre_w	Sen_o	Sen_w	$DPre$	$DSen$
Random	$\leq 50k$	88.67	88.16	92.60	93.25	0.51	0.65
Forest	$> 50k$	74.96	76.06	65.16	63.14	1.10	2.02
Decision	$\leq 50k$	87.20	87.00	87.28	87.05	0.20	0.23
Tree	$> 50k$	62.45	61.82	62.29	61.70	0.63	0.59
SVM	$\leq 50k$	86.43	86.48	94.34	94.36	0.05	0.02
	$> 50k$	77.19	77.32	56.41	56.60	0.13	0.19
AdaBoost	$\leq 50k$	87.92	87.84	94.25	94.51	0.08	0.26
	$> 50k$	78.52	79.21	61.90	61.50	0.69	0.40

图 6 和图 7 显示了 ANDW 对原始数据库进行数据脱敏并嵌入水印后两个敏感属性列 ('age' 和 'hour_per_week') 的直方图分布情况, 由图可知, ANDW 的数据分布与原始数据库具有极高的相似度, 不会影响使用者对数据库进行特征分析。

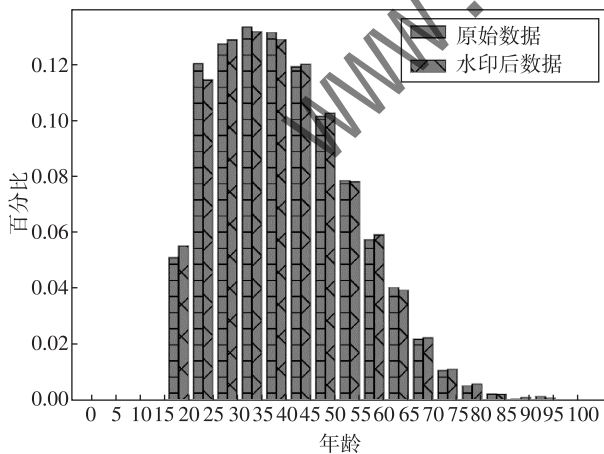


图 6 嵌入水印前后属性列 'age' 的直方图分布情况

3.3 水印提取鲁棒性分析

为了提高水印算法的鲁棒性, ANDW 在提取水印时采取投票原则, 根据提取出的水印信息位中出现频次较高的比特位 (0 or 1) 来确定分组或频次中嵌入的水印位。

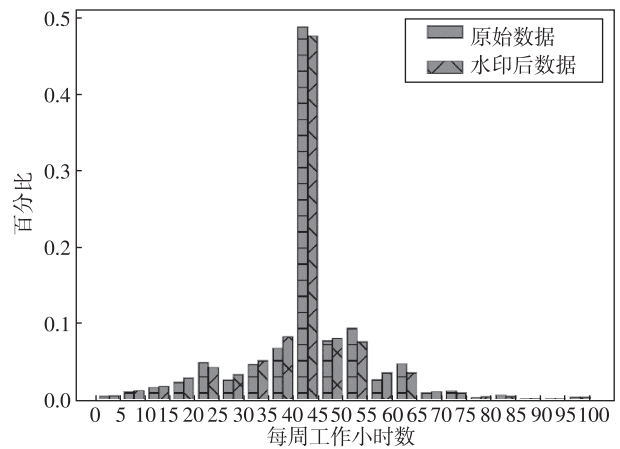


图 7 嵌入水印前后属性列 'hour_per_week' 的直方图分布情况

本小节实验使用误码率 (Bit Error Rate, BER) 来评估水印的鲁棒性。实验模拟攻击者对带水印的数据库中的元组随机执行插入、修改和删除操作, 分别改变 $per = 10\%$, 20% , 30% , ..., 90% 的数据, 然后从受到攻击后的数据库中提取水印, 计算 BER。

对于插入攻击, 由于主键的唯一性, 在水印提取阶段的数据预处理时, 可以通过主键信息排除掉攻击者随机插入的元组, 因此无论插入多少数据, 水印提取的 BER 始终为 0。

图 8 显示了 ANDW 在受到修改和删除攻击时的鲁棒性表现。实验结果表明, 在修改攻击时, 当修改率 $per \leq 80\%$ 时, ANDW 的 BER 始终为 0, 在 $per > 80\%$ 后, BER 也非常小, 仅为 1.88%。而在删除攻击时, ANDW 方法的 BER 始终为 0, 从理论上分析, 在删除数据时只有当攻击者将每个分组中嵌入部分的数据全部删除, 才有 50% 的概率会影响到最终提取出的水印位, 在数据库容量非常大时, 这种情况很难出现, 因此 ANDW 对于删除攻击表现出极强的鲁棒性。以上说明 ANDW 是一种高度

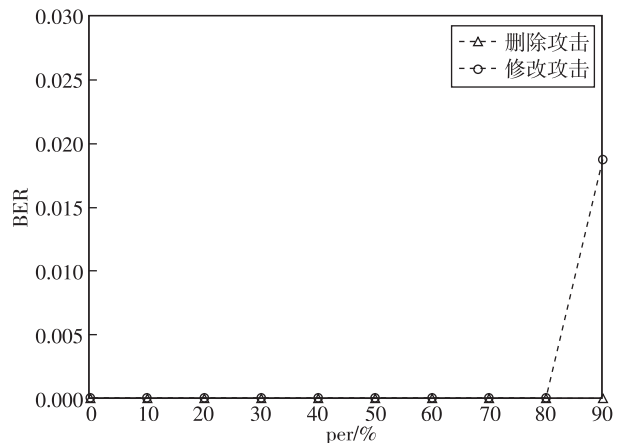


图 8 修改和删除攻击时水印提取的 BER

鲁棒的数据库脱敏和水印方案。

3.4 时间复杂度分析

ANDW 方案由三个阶段组成: 数据预处理、水印嵌入、水印提取。其中数据预处理阶段主要进行数据库分组和水印信息生成, 数据库分组的时间复杂度为 $O(R \times A)$, 水印信息生成主要进行基于一维 Logistic 的置乱算法, 其时间复杂度为 $O(N_g \times \log N_g)$, 其中 R 为数据库的总元组数, A 为数据库的敏感属性列数, N_g 为水印长度。在水印嵌入阶段, 其时间复杂度同样为 $O(R \times A)$ 。在水印提取阶段, 需要进行数据库分组、水印提取和对水印执行逆置乱算法, 其中数据库分组的时间复杂度与预处理时一致, 逆置乱算法的时间复杂度与置乱算法一致, 而水印提取时间复杂度与水印嵌入阶段一致。并且由于水印信息长度通常远小于数据库元组数, 因此 ANDW 方案的时间复杂度为 $O(R \times A)$ 。

4 结论

本文提出了一种基于加性噪声的强鲁棒数据库盲水印方法 (ANDW)。实验结果表明, ANDW 方法可以在不影响数据脱敏的隐私保护性能的前提下, 实现数据库水印的盲提取, 并具有极强的鲁棒性, 在数据库遭受非常恶劣的攻击后也能以极高的准确率恢复出原始水印信息。该方法对数据造成的失真很小, 保留了数据可用性以及与原始数据库类似的统计特征。因此, ANDW 方法是一种集成式的强鲁棒性数据库盲水印与数据脱敏方法, 解决了大数据在共享与发布过程中面临的个人隐私数据保护、泄密溯源与版权保护问题。

未来工作中将进一步设计构建更加全面的数据脱敏与数据库水印方案, 实现敏感数据自适应识别, 并区分不同类型的数据和不同程度的脱敏级别, 自适应选择相应算法。

参考文献

- [1] ADHIKARI K, PANDA R K. Users' information privacy concerns and privacy protection behaviors in social networks [J]. Journal of Global Marketing, 2018, 31 (2): 96–110.
- [2] WIERINGA J, KANNAN P, MA X, et al. Data analytics in a privacy-concerned world [J]. Journal of Business Research, 2021, 122: 915–925.
- [3] KHANDUJA V. Database watermarking, a technological protective measure: perspective, security analysis and future directions [J]. Journal of Information Security and Applications, 2017, 37: 38–49.
- [4] LI T C, LI N H. On the tradeoff between privacy and utility in data publishing [C]//Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2009: 517–526.
- [5] 冯登国, 张敏, 李昊, 等. 大数据安全与隐私保护 [J]. 计算机学报, 2014, 37 (1): 246–258.
- [6] FRANCO-CONTRERAS J, COATRIEUX G. Robust watermarking of relational databases with ontology-guided distortion control [J]. IEEE Transactions on Information Forensics and Security, 2015, 10 (9): 1939–1952.
- [7] AGRAWAL R, KIERNAN J. Watermarking relational databases [C]//Proceedings of the 28th International Conference on Very Large Databases, 2002: 155–166.
- [8] ZHANG Y X, WANG Z H, WANG Z G, et al. A robust and adaptive watermarking technique for relational database [C]//China Cyber Security Annual Conference, 2021: 3–26.
- [9] REN Z, FANG H, ZHANG J, et al. A robust database watermarking scheme that preserves statistical characteristics [J]. IEEE Transactions on Knowledge and Data Engineering, 2023, 36 (6): 2329–2342.
- [10] GUO J. Fragile watermarking scheme for tamper detection of relational database [C]//2011 International Conference on Computer and Management (CAMAN), 2011: 1–4.
- [11] BHATTACHARYA S, CORTESI A. Database authentication by distortion free watermarking [C]//ICSOFT, 2010: 219–226.
- [12] WANG H, CUI X, CAO Z. A speech based algorithm for watermarking relational databases [C]//2008 International Symposiums on Information Processing, 2008: 603–606.
- [13] SION R, ATALLAH M, PRABHAKAR S. Rights protection for categorical data [J]. IEEE Transactions on Knowledge and Data Engineering, 2005, 17 (7): 912–926.
- [14] CAMARA L, LI J Y, LI R F, et al. Distortion-free watermarking approach for relational database integrity checking [J]. Mathematical Problems in Engineering, 2014, 2014: 1–10.
- [15] AIHAB K, AFAQ H S. A fragile zero watermarking scheme to detect and characterize malicious modifications in database relations [J]. The Scientific World Journal, 2013. DOI: 10.1105/2013/796726.
- [16] ADAM N R, WORTHMAN J C. Security-control methods for statistical databases: a comparative study [J]. ACM Computing Surveys (CSUR), 1989, 21 (4): 515–556.
- [17] MURTHY S, BAKAR A A, RAHIM F A, et al. A comparative study of data anonymization techniques [C]//2019 IEEE 5th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS), 2019: 306–309.
- [18] SARADA G, ABITHA N, MANIKANDAN G, et al. A few new approaches for data masking [C]//2015 International Conference on Circuits, Power and Computing Technologies, 2015: 1–4.

(下转第 43 页)

- [9] 袁进良. 面向移动终端的资源高效联邦学习方法研究 [D]. 北京: 北京邮电大学, 2019.
- [10] 张连福. 联邦学习隐私保护关键问题研究 [D]. 南昌: 江西财经大学, 2023.
- [11] 张旭. 基于差分隐私机制的数据隐私保护的研究 [D]. 南京: 南京邮电大学, 2023.
- [12] 王伟艳. 基于同态加密的安全多方计算协议的优化与应用 [D]. 太原: 中北大学, 2023.
- [13] 李建华, 银鹰, 李思源, 等. 大数据安全与隐私计算技术综述 [J/OL]. 网络空间安全科学学报, 1 - 15 [2024 - 12 - 18]. <https://doi.org/10.20172/j.issn.2097-3136.240601>.
- [14] 戴怡然, 张江, 向斌武, 等. 全同态加密技术的研究现状及发展路线综述 [J]. 电子与信息学报, 2024, 46 (5): 1774 - 1786.
- [15] Adult; UCI machine learning repository [DB/OL]. [2024 - 10 - 18]. <https://doi.org/10.24432/C5XW20>. (收稿日期: 2024 - 12 - 18)

作者简介:

李思慧 (1985 -), 女, 硕士, 工程师, 主要研究方向: 大数据、人工智能。

戴明超 (1989 -), 男, 硕士, 助理工程师, 主要研究方向: 大数据、人工智能。

蔡伍洲 (1989 -), 男, 本科, 工程师, 主要研究方向: 大数据、人工智能。

(上接第 38 页)

- [19] GOSWAMI P, MADAN S. Privacy preserving data publishing and data anonymization approaches: a review [C]//2017 International Conference on Computing, Communication and Automation (ICCCA), 2017: 139 - 142.
- [20] MARQUES J F, BERNARDINO J. Analysis of data anonymization techniques [C]//KEOD, 2020: 235 - 241.
- [21] BERTINO E, OOI B C, YANG Y J, et al. Privacy and ownership preserving of outsourced medical data [C]//21st International Conference on Data Engineering (ICDE' 05), 2005: 521 - 532.
- [22] NAKAMURA Y, NAKATSUKA Y, NISHI H. Novel method to watermark anonymized data for data publishing [J]. IEICE Transactions on Information and Systems, 2017, 100 (8): 1671 - 1679.
- [23] NAKAMURA Y, NISHI H. Digital watermarking for anonymized data with low information loss [J]. IEEE Access, 2021, 9: 130570 - 130585.
- [24] BORDEL B, ALCARRIA R, ROBLES T, et al. Data authentication and anonymization in IoT scenarios and future 5G networks using chaotic digital watermarking [J]. IEEE Access, 2021, 9: 22378 - 22398.
- [25] YU J, YUAN S G, YUAN Y L, et al. A k-anonymity-based robust watermarking scheme for relational database [C]//Science of Cyber Security: 4th International Conference, SciSec 2022, 2022: 557 - 573. (收稿日期: 2024 - 12 - 01)

作者简介:

李程 (1994 -), 通信作者, 男, 硕士, 助理工程师, 主要研究方向: 数据安全、隐私保护。E-mail: licheng2021@alumni.pku.edu.cn。

张国栋 (1995 -), 男, 本科, 助理工程师, 主要研究方向: 信息安全。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部

www.pcachina.com