Computer Development and Applications 计算机发展与应用, 2025, 3(2), 1-5
Published Online June 2025.
http://www.ufascience.com/journal.aspx?ProID=2

保护数据隐私的扰动方法：技术与应用综述

吴斌

大连理工大学，大连 116024，中国

摘要：扰动方法是一种数学技术，用于向数据添加受控噪声或随机性，以在允许数据分析的同时保护隐私。各种方法，例如随机响应、差异隐私、安全多方计算、噪声添加以及采样和聚合，都用于保护敏感信息免遭泄露或利用。这些方法已成功应用于机器学习、统计学和密码学，以确保数据隐私。然而，它们的实现必须经过精心设计，以避免损害数据准确性或在分析中引入偏差。大多数情况下，扰动方法为保护各个领域的数据隐私提供了一种有前途的方法。本综述概述了用于保护各个领域的数据隐私的扰动方法，包括机器学习、统计学和密码学。扰动方法涉及向数据添加受控噪声或随机性以保护隐私，同时仍允许数据分析。

关键词：隐私；保护隐私的数据挖掘；大数据；多维网格；隐私增强；扰动方法

Perturbation Methods for Protecting Data Privacy: A Review of Techniques and Applications

Bin Wu

Dalian University of Technology, Dalian 116024, China

Abstract: Perturbation methods are mathematical techniques used to add controlled noise or randomness to data to protect privacy while allowing data analysis. Various methods, such as randomized response, differential privacy, secure multi-party computation, noise addition, and sampling and aggregation, are used to protect sensitive information from disclosure or exploitation. These methods have been successfully applied in machine learning, statistics, and cryptography to ensure data privacy. However, their implementation must be carefully designed to avoid compromising data accuracy or introducing bias in analysis. Mostly, perturbation methods offer a promising approach to protect data privacy in various fields. This review provides an overview of perturbation methods used to protect data privacy in various fields, including machine learning, statistics, and cryptography. Perturbation methods involve adding controlled noise or randomness to data to preserve privacy while still allowing data analysis.

Keywords: Privacy; Data mining protecting privacy; Big data; Multi-dimensional grid; Privacy enhancement; Perturbation approach

个人和组织产生的数字数据量日益增长，引发了人们对敏感信息隐私和安全的担忧。未经授权访问个人数据可能导致身份盗窃、金融欺诈和其他恶意活动。数据隐私是一个至关重要的问题，尤其是对于包含个人或机

文章引用: 吴斌. 保护数据隐私的扰动方法：技术与应用综述[J]. 计算机发展与应用, 2025, 3(2): 1-5.
DOI: .

密信息的敏感数据。扰动方法是一组数学技术，可以通过在数据中添加受控噪声或随机性来保护数据隐私，同时仍允许数据分析。这些方法可以应用于机器学习、统计学和密码学等各个领域，以防止攻击者识别个人或敏感信息。本综述概述了用于保护数据隐私的扰动方法，包括其优缺点，以及谨慎实施以确保准确性和防止偏见的重要性。

在当今信息时代，随着组织收集和存储大量个人数据，数据隐私已成为一个关键问题。虽然数据分析可以提供有价值的见解并改进决策，但它也对个人隐私构成风险。扰动方法提供了一种在保护数据隐私的同时仍允许数据分析的有前途的方法。这些方法涉及向数据添加受控噪声或随机性以保护隐私。在本综述中，

我们将概述用于保护数据隐私的扰动方法，包括随机响应、差分隐私、安全多方计算 (SMC)、噪声添加以及采样和聚合。我们还将讨论这些方法的优势和局限性，以及它们在各个领域的潜在应用。通过了解可用于数据隐私保护的各种扰动方法，研究人员和从业人员可以就如何在保护敏感信息的同时仍允许进行数据分析做出明智的决策。

一、文献综述

目前已有大量关于用于保护数据隐私的扰动方法的研究。以下文献综述重点介绍了该领域各类研究的一些关键发现和贡献：

(1) 随机响应：该技术为调查或问卷中个人的回答增加了随机性，使攻击者难以确定真实回答 [1]。Warner 于 1965 年首次提出该方法，用于保护调查中的个人隐私 [2]。此后，该方法已广泛应用于医疗保健、社会科学和市场营销等各个领域。Ghosh 和 Roth 的一项研究提出了一种广义随机响应方法，该方法比原始方法提供了更好的隐私保障 [3]。

(2) 差分隐私：它向数据中添加随机噪声，以防止攻击者识别个人。该技术可应用于多种数据分析技术，例如机器学习、统计学和数据挖掘。Dwork 等人首次提出了隐私保护方法 [6]。此后，它已成为保护敏感信息的流行方法。Wang 等人提出了一种用于深度学习模型的差分隐私算法，该算法比现有方法提供了更强的隐私保障 [4]。差分隐私中最常见的噪声类型是拉普拉斯机制、指数机制和高斯机制。它们通过向原始数据条目添加噪声来工作，并且可以应用于实数特征和分类特征。

(3) 安全多方计算 (SMC)：SMC 已广泛应用于隐私保护数据分析，其中将来自不同来源的数据组合起来进行联合分析。Chaum 等人的一项研究提出了一种使用 SMC 进行统计函数安全计算的实用方法 [5]。Lindell 和 Pinkas 提出了一种实用的 SMC 协议，该协议广泛应用于各种应用 [6]。

(4) 噪声添加：此技术涉及在发布数据进行分析之前向数据中添加少量随机噪声。一些研究人员提出了一种基于噪声添加的隐私保护主成分分析方法，该方法在保持数据效用的同时，确保数据隐私性 [7]。

(5) 采样和聚合：采样涉及选择要分析的数据子集，而聚合涉及组合来自多个来源的数据进行分析。这些技术可用于降低敏感信息泄露的风险，同时仍能进行准确的数据分析 [8]。该方法的有效性已在包括数据挖掘和机器学习在内的各种应用中得到研究。

(6) 隐私保护机器学习：本文探讨了机器学习算法相关的隐私风险，并提出了各种扰动方法来保护机器学习中的数据隐私。作者讨论了每种方法的优缺点，并重点介绍了它们在机器学习中的应用。

(7) 隐私保护数据挖掘：Charu 等人概述了各种扰动方法，包括差分隐私、随机化和安全多方计算。

除了这些方法之外，其他扰动技术也被提出，包括数据交换、数据脱敏和 k 匿名。这些技术已在各种应用中得到研究，并在保护数据隐私方面展现出良好的效果。

二、模型与分析

扰动方法取决于具体的数据分析任务和所需的隐私保护级别。差分隐私提供了强大的隐私保障，但计算成本可能较高，并且会导致数据准确性降低。随机响应和噪声添加在隐私和准确性之间提供了可调整的权衡，但可能无法提供针对更复杂攻击的强大隐私保护。采样和聚合具有计算效率，并且可以轻松应用于大型数据集，但可能无法提供针对更复杂攻击的强大隐私保护。精心设计和实施这些方法非常重要，以确保它们不会损害数据准确性或在结果中引入偏差。

本节将讨论数据扰动-旋转扰动；主成分分析 (PCA)；投影扰动；几何数据扰动；数据交换；数据随机化；启发式数据隐私保护方法；k-匿名性；k-匿名性 l-多样性；k-匿名性 l-接近性；个性化隐私保护；基于效用的隐私保护；密码方法；安全多方计算；水平划分数据；并给出了垂直划分数据方法的说明。

主成分分析 (PCA) 中的旋转扰动是一种在保留数据整体结构的同时向主成分添加噪声或扰动的技术。它涉及旋转主成分并对旋转后的成分进行扰动。

PCA 中旋转扰动的具体公式可能涉及其他考虑因素，具体取决于所选的扰动方法和所需的扰动程度。目标是在保留数据整体结构和统计特性的同时引入噪声。选择合适的扰动参数和技术，以平衡扰动数据中的隐私保护和数据效用至关重要。

投影扰动是一种在保留某些统计属性的同时，向数值数据添加噪声或扰动的技术。它涉及将数据投影到低维空间并对投影值进行扰动。投影扰动的具体公式取决于所使用的扰动方法。

数据扰动和投影扰动是数据科学和机器学习中常用的两种数据隐私保护技术。数据扰动涉及向数据添加随机噪声，以保护单个数据点的隐私。添加的噪声水平可以通过隐私预算来控制，从而平衡隐私保护和数据效用。另一方面，投影扰动涉及将数据投影到低维空间，同时向投影中添加噪声。该技术有助于去除数据的识别性特征，同时保留数据点的整体结构和关系。方法的选择取决于具体的应用和隐私需求。此外，应谨慎选择所使用的噪声或降维级别，以平衡隐私保护和数据效用。

几何数据扰动是一种向几何数据添加噪声或扰动的技术，旨在保护隐私的同时保留数据的总体形状或结构。几何数据扰动的具体公式可能因所使用的扰动方法而异。

数据交换是一种隐私保护技术，用于在保留数据统计属性的同时保护敏感信息。它涉及在数据记录之间交换或交换值，其方式是保持整体数据分布不变，但会模糊各个记录之间的原始关系。数据交换的具体公式取决于所使用的交换方法。

基于 k 匿名性的交换公式涉及在集群中选择合适的记录并交换敏感属性的值。确切的实现可能因用于 k-匿名的具体算法而异。

数据随机化是一种通过在原始数据值中引入随机噪声或扰动来保护数据隐私的技术。数据随机化的具体公式取决于所使用的随机化方法。

随机噪声通常由特定分布生成，隐私参数控制所提供的隐私保护级别。

启发式方法在数据科学和机器学习中常用于保护数据隐私。这些方法涉及使用通用的问题解决技术来制定保护敏感数据的策略和规则。

启发式数据隐私方法的一个例子是 k-匿名性，它是一种用于确保数据集中每条记录与数据集中至少 k-1 条其他记录无法区分的技术。这涉及将相似的记录分组在一起，并删除任何可用于将记录与特定个人联系起来的识别信息。

另一个例子是 l-多样性，它是一种用于确保具有给定敏感属性值的每组记录对于另一个属性至少具有 l 个不同值的技术。这有助于防止攻击者将敏感属性与数据集中的特定个体关联起来。其他用于数据隐私的启发式

方法包括 t 值接近度、差分隐私以及基于机器学习的技术，例如生成对抗网络 (GAN) 和变分自编码器 (VAE)。虽然启发式方法可以有效保护数据隐私，但务必仔细评估其有效性，并根据具体的分析需求和与数据相关的隐私风险选择合适的方法和参数。

k-匿名是一种隐私保护技术，旨在保护数据集中的个人身份，确保数据集中的每条记录在某些识别属性方面与至少 k-1 条其他记录无法区分。k-匿名原则通过降低个人身份信息的唯一性来帮助防止个人身份被重新识别。k-匿名的基本思想是泛化或抑制属性值，使记录组变得无法区分，同时保持数据的整体统计属性。实现 k-匿名的具体公式取决于所选的泛化或抑制方法。

需要注意的是，实现 k-匿名需要仔细考虑所选的属性、泛化或抑制的级别以及所需的隐私保护级别。此外，k-匿名的有效性取决于所应用的泛化或抑制技术的质量以及匿名组的规模。在实施 k-匿名性时，在隐私保护和数据效用之间取得平衡至关重要，这样才能既能保护隐私，又能对匿名数据进行有意义的分析。

k-匿名性旨在通过确保数据集中的每条记录与至少 k-1 条其他记录无法区分来保护个人身份。然而，仅靠 k-匿名性可能不足以防止属性泄露。这时，l-多样性作为 k-匿名性的增强功能应运而生。l-多样性确保每组无法区分的记录（基于 k-匿名性）包含至少 l 个敏感属性的良好表示值。

实现 l-多样性的具体公式取决于所选方法和良好表示值的定义。

l-多样性背后的关键思想是确保在每个组中，敏感属性具有足够数量的独特且具有良好代表性的值，以防止属性泄露，即使基于 k-匿名性仍然无法区分该组。

k-匿名和 l-接近性是两种互补的隐私保护技术，用于保护数据集中的敏感信息。k-匿名侧重于隐藏个人身份，而 l-接近性则旨在通过确保一组记录中的敏感属性具有足够的多样性来解决属性泄露问题。在组内实现 l-接近性的具体公式取决于所选的具体距离或相似性度量以及所选的数据转换技术。目标是确保组内的敏感属性值表现出满足 l-接近性要求的多样性。通过结合 k-Anonymity 和 l-Closeness，可以加强隐私保护，因为 k-Anonymity 确保记录的不可区分性，而 l-Closeness 通过强制每个组内的多样性来解决属性泄露的风险。

个性化隐私保护 (P3) 是一种启发式数据隐私保护方法，其侧重于保护个人隐私而非整体数据集的隐私。P3 的目标是使数据分析师能够从数据集中提取有用信息，同时最大限度地降低泄露个人敏感信息的风险。为了实现 P3，数据集中的每个个体都被分配一个个性化隐私参数，该参数决定了他们所获得的隐私保护级别。该参数基于个体身份泄露的风险，该风险是根据其属性在数据集中的独特性计算得出的。属性独特性较高的个体获得更高级别的隐私保护，而属性独特性较低的个体获得较低级别的保护。个性化隐私保护是指根据数据主体的个人偏好和需求定制隐私保护机制的概念。它旨在让用户能够控制自己的个人信息，同时仍然能够从数据分析和服务中获益。

基于效用的隐私保护是一种启发式方法，通过平衡隐私保护与数据的效用（或有用性）来保护数据隐私。该方法认识到，完全的隐私保护并非总是可行或可取的，尤其是在需要数据用于研究或其他目的的情况下。为了实施基于效用的隐私保护，首先需要评估数据，根据数据的敏感性和数据泄露的风险确定所需的隐私保护级别。然后，对数据进行处理，以确保隐私保护应用于适当的数据元素，同时最大限度地降低对数据效用的影响。在基于效用的隐私保护中，重点在于优化数据隐私与数据效用之间的权衡。

密码学方法是一类用于保护数据隐私的启发式方法，它涉及使用加密和解密技术来保护敏感数据。这些方法使用数学算法对数据进行编码，使得只有拥有适当解密密钥的授权个人或系统才能访问数据。它们大致可分为两类：对称密钥加密和公钥加密。一种常用的数据隐私保护方法是对称密钥加密，其中加密和解密使用相同的密钥。在这种方法中，数据使用数据所有者和授权接收者共享的密钥进行加密。然后，数据通过网络安全地

传输或存储在设备上，并且只有拥有适当解密密钥的人才能访问。另一种用于数据隐私保护的方法是公钥加密，其中使用两个不同的密钥进行加密和解密。在这种方法中，公钥用于加密数据，而私钥用于解密。

在 MPC 协议中，各方持有各自的私有数据，并希望在不与其他方共享数据的情况下，基于合并后的数据计算函数。为了实现这一点，各方需要相互交互，以保护隐私的方式执行计算。

MPC 背后的关键理念是，即使各方贡献了各自的私有输入和部分计算，也没有任何一方能够确定其他方的输入或中间结果。该协议确保整个计算过程中输入的隐私性、机密性和完整性。

水平数据分区是一种数据隐私技术，用于在保护隐私的同时，跨多个数据源分发和存储不同的属性或数据子集。

垂直数据分区是一种数据隐私技术，用于根据不同的属性或列将数据集垂直拆分为多个子集。每个子集包含原始属性的子集，从而保护某些敏感属性的隐私。垂直划分数据的具体公式取决于所使用的隐私保护技术以及数据集的具体属性和隐私要求。可以采用各种算法和方法来确定最佳划分策略并实现所需的隐私保障。

三、结论

总而言之，有多种扰动方法可用于保护数据隐私，每种方法都有其优缺点。随机响应和噪声添加是简单有效的扰动方法，但它们可能容易受到某些类型的攻击，并且可能需要仔细调整噪声水平以平衡隐私保护和数据效用。差分隐私提供了强大的隐私保障，但计算成本较高。安全多方计算无需扰动或修改数据即可提供强大的隐私保护，但计算成本也可能较高。

扰动方法的选择取决于具体应用以及隐私保护和数据效用之间的权衡。研究人员正在持续探索和开发新的扰动方法和优化技术，以在各种环境下提高数据分析的隐私性和效用。

参考文献

[1] Newman M E J. The structure and function of complex networks, SIAM Rev, 2023, 45(2): 167-256.
[2] Kargupta Hillol, Datta Souptik, Wang Q, et al. On the privacy preserving properties of random data perturbation techniques. Proceedings - IEEE International Conference on Data Mining, ICDM, 2023: 99- 106.
[3] Warner SL. Randomized response: a survey technique for eliminating evasive answer bias. Journal of the American Statistical Association, 1965, 60(309): 63-69.
[4] Ghosh A, Roughgarden T, Sundararajan M. Universally utility-maximizing privacy mechanisms. SIAM J. Computer, 2012, 41(6): 1673-1693.
[5] Xu L, Jiang J, Wang J, et al. Information Security in Big Data: Privacy and Data Mining. IEEE Access, 2014(2): 1149–1176.
[6] Dwork C, McSherry F, Nissim K, et al. Calibrating noise to sensitivity in private data analysis. In Theory of Cryptography Conference. Springer: Berlin/Heidelberg, Germany, 2006: 265–284.
[7] Wang T, Zheng Z, Rehmani MH, et al. Privacy Preservation in Big Data from the Communication Perspective—A Survey. IEEE Communications Surveys and Tutorials, 2019, 21: 753–778.
[8] Liu C, Chen S, Zhou S, et al. A novel privacy preserving method for data publication. 2019. DOI: 10.1016/j.ins.2019.06.022.