数据库实训平台信息隐私加密方法设计

付思思 [1]
FU Sisi

摘 要 常规的隐私加密方法未能充分考虑密文长度的限制，容易导致加密结果超出预期范围，增加了信息泄露的风险，对数据机密性和完整性造成潜在威胁。为此，提出一种数据库实训平台信息隐私加密方法。根据数据库实训平台中的数据信息格式，将数据维度处理成为一维向量的形式，利用 Logistic 映射分类集成平台中的隐私数据信息。使用近似同态比较分析计算隐私信息密文长度区间阈值，约束密文长度在合理范围内。在区间阈值约束下为集成的信息添加相应的密文，确保在加密过程中对密文长度进行有效限制，实现信息隐私加密。经过实验可知，依据所提出方法能够有效分类集成数据，密钥未超过区间阈值，得出的隐私加密结果 Lyapunov 指数较大，加密后的信息安全性较优，满足了数据库实训平台信息的安全保障需求。

关键词 数据库；实训平台；信息加密；隐私加密；加密方法

doi：10.3969/j.issn.1672-9528.2024.05.042

0 引言

为了有效利用数据库的信息化功能，许多单位都开设了数据库相关的实训课程。数据库实训平台具有支持多种类型数据库及其基本操作的优势，可以满足实际培训内容对数据库实训环境的需求，逐渐得到了广泛应用 [1]。然而，在数据库实训平台的实践应用过程中，平台中存在着大量的用户个人信息，包括教师、学生以及管理人员等多方面的隐私信息。这些信息不仅涉及了姓名、地址、电话号码、身份证号码等敏感信息，还涉及了数据库实训素材内容的隐私敏感信息。在这样的情况下，通过加密防止数据库实训平台中的用户隐私信息被非法获取成为该平台在实践应用过程中的研究重点。

为了应对该问题，在当前的研究中，宋永占等人 [2] 在平台中挖掘用户的个人隐私相关数据，利用隐藏分类算法对电网隐私数据进行多层级加密。该方法未能充分考虑密文长度的限制，在多层级加密过程中，攻击者可能通过分析超长密文获得更多关键信息。姜春峰等人 [3] 提出属性分类下分布式数据隐私保护加密方法，对分布式数据的结构特征进行分析，从而针对该特征所对应的属性类型，为其添加隐私保护密钥，完成隐私信息加密。由于该方法未充分考虑密文长度限制，加密结果的长度超出预期范围，导致加密强度下降。超长密文可能意味着密钥空间不能提供足够的混淆和保护，从而削弱了加密算法的安全性，使得数据更容易受到攻击和破解。Ghosal 等人 [4] 首先利用 Lah 变换为隐私信息生成多项式序列，转换到变换域中，然后设计该数据所需的隐藏度，进而设计相应的、更加具有指向性的数据加密方案。在该方法中，未提及对密文长度的控制策略，可能使加密系统缺乏必要的安全机制。缺乏明确的密文长度控制，导致加密过程缺乏有效性和可靠性。Yao 等人 [5] 提出基于云计算的隐私信息反篡改加密方法，通过大数据分析、实验研究、变量比较等方法对隐私信息进行反窃取控制加密。该方法在反扒取控制加密过程中未考虑密文长度的限制，过长的密文会导致加密和解密的效率下降。密文过长会增加计算和处理资源的消耗，降低系统的性能表现，尤其是在云计算场景下可能影响整个系统的吞吐量和响应速度，导致加密结果安全性不理想。

针对以上隐私加密保护方法未充分考虑密文长度限制，在隐私信息加密过程中带来密文长度超出预期、信息泄露风险增加、加密性能下降等问题，本研究针对数据库实训平台中信息的运行环境，提出一种信息隐私加密方法。该方法通过分析数据库实训平台中的隐私性质，将数据维度处理成为一维向量的形式。利用 Logistic 映射将平台中的数据信息分类为需要隐私加密处理的隐私信息以及非隐私信息，在此基础上，通过计算隐私信息密文长度的区间阈值，约束密文长度在合理范围内。在区间阈值的约束下，为集成信息添加相应的密文，实现加密过程，从而提高数据库实训平台中信息的隐私保护水平。

1. 江西现代职业技术学院 江西南昌 330095

[基金项目]2022 年度江西省教育厅科学技术研究项目（GJJ2205123）

1 数据库实训平台信息隐私加密方法设计

1.1 Logistic 映射下隐私数据分类集成

基于数据库实训平台中所包含的数据信息中存在常规的平台运行数据，这些数据并不在隐私加密的范围内，如果与隐私信息一起进行加密，将增加工作量，降低隐私防护效果。为此，本研究利用 Logistic 映射对数据库实训平台中的隐私数据信息和非隐私数据信息进行分类处理。通过降维处理将原始的实训平台数据信息较为杂乱的存储态势，转变成为隐私数据信息和非隐私数据信息分类集成的存储态势。分析数据库实训平台中的数据信息格式，如图 1 所示。

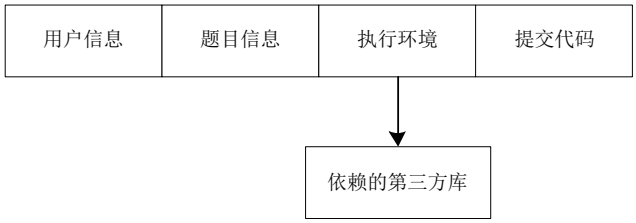

图 1 数据库实训平台数据信息格式

根据如图 1 所示的数据信息格式，本研究采用 Logistic 映射的方法将实训平台中的隐私数据信息进行分类集成。首先，将实训平台中的数据信息降维处理成为 Logistic 映射可处理的一维形式。然后，构建数据信息的协方差矩阵，在该矩阵中，定义矩阵对角线为数据信息的维度。最后，在此基础上，求解平台数据信息在该矩阵中的一维向量，其公式为：

$$Z=\frac{\Lambda^{z}}{V^{T}} \tag{1}$$

式中：$\boldsymbol{Z}$ 表示平台数据信息的一维向量，z 表示数据信息的非零特征值，$\boldsymbol{T}$ 表示对角矩阵，$\boldsymbol{\Lambda}$ 表示数据信息的协方差矩阵，V 表示最大特征值。

通过公式（1）求解得到的平台数据一维向量，将其处理成为一维的数据形式。利用处理后的数据信息，构建 Logistic 映射的数学模型，其公式 [6] 为：

$$x=x_{Z}\times\mu\times(1-v) \tag{2}$$

式中：x 表示 Logistic 映射数学模型，x_Z 则表示一维向量 Z 在数学模型中的初值，μ 表示控制参数，v 表示斜率。

在本研究中，根据数学模型中实训平台的数据信息一维向量特性，将控制参数阈值设定为 4，在该数值下，解析一维向量数据信息在 Logistic 映射数学模型中的倍周期分岔图，如图 2 所示。在控制参数阈值设定为 4 的状态下，平台一维向量数据信息在 Logistic 映射数学模型中，呈现出了不同的混沌值。当控制参数在 1.5 ~ 2.26 的区间时，信息在数学模型中仅存在一个混沌点，并且该混沌点在模型中的输出为“0”；当控制参数在 2.26 ~ 3.0 的区间内时，信息在数学模型中仍然仅存在一个混沌点，但该混沌点所对应的模型输出值不再为“0”，而是呈现出稳定上升的状态，本研究将该状态作为平台数据信息在模型的周期一解；当控制参数在阈值内继续增加后，所对应的模型输出值将出现倍周期分叉的现象，平台数据信息在模型中不再仅有一个混沌点，本研究将该状态作为平台数据信息在模型的周期二解；当控制参数在 3.35 ~ 4.0 的区间内时，信息在数学模型中的输出值进入混沌区，呈现出完全的混沌状态，本研究将该状态作为平台数据信息在模型的周期三解。

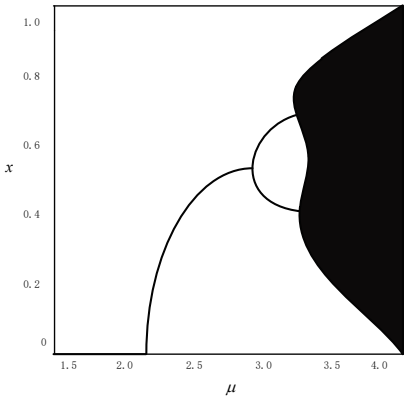

图 2 倍周期分岔图

根据图 2 对 Logistic 映射混沌不同周期解序列的分析结果，利用公式（2）Logistic 映射数学模型的输出结果，计算数据库实训平台中隐私数据信息和非隐私数据信息的混沌映射值，其公式为：

$$R(x)=-\alpha x_{n}(\hat{\mu}-\frac{x}{\alpha}) \tag{3}$$

式中：$R(x)$ 表示 Logistic 映射数学模型输出值 x 的混沌映射值，α 表示常数，n 表示 Logistic 映射混沌周期的解序列，$\hat{\mu}$ 表示控制参数的单峰值。

基于公式（3）计算所得的混沌映射值，对实训平台中的隐私信息及非隐私信息进行分类集成。隐私信息的分类集成结果为：

$$H(i)=\varphi\sum_{i=1}^{n}\chi_{i}(R(x)_{1},R(x)_{2}) \tag{4}$$

式中：i 表示分类集成的实训平台隐私数据信息，$H(i)$ 表示该信息的分类集成结果，φ 表示隐私信息的初始敏感值，χ 表示隐私阈值，$R(x)_1$ 和 $R(x)_2$ 分别表示平台隐私信息和非隐私信息的混沌映射值。

通过上述步骤，将数据库实训平台中的数据信息按照隐私性及非隐私性进行分类集成处理，为后续隐私提供良好数据基础。

1.2 基于近似同态比较计算隐私信息密文长度区间阈值

基于上节分类集成得到的数据库实训平台隐私数据信息，将其单独提取到平台的存储单元中，与非隐私的平台数

据信息分类，针对性地进行后续隐私加密过程。

根据提取得到的数据库实训平台隐私数据信息，本研究对其所需的密文长度区间进行分析计算。本研究采用近似同态比较的方法分析其信息隐私明文复杂度。构建近似同态比较的比较函数，其公式[7]为：

$$C(a,b)=\lim_{k\to\infty}\frac{a_k}{a_k+b_k} \tag{5}$$

式中：a 和 b 分别表示 $H(i)$ 中两个随机数据信息，$a\in H(i)$，$b\in H(i)$；$C(a,b)$ 表示两个数据信息的比较函数；k 表示项式；a_k 和 b_k 则分别表示 a 和 b 的多项式。

根据该比较函数，分析两个数据信息的近似值。近似值的定义为：

$$C(a,b)=\begin{cases}1, a>b\\ \frac{1}{2}, a=b\\ 0, a<b\end{cases} \tag{6}$$

基于如公式（6）所示的定义，为实训平台的隐私数据信息添加近似值的属性标签。利用该属性标签，计算相应数据信息的log级明文复杂度[8]。本研究以隐私数据信息 a 为例，其明文复杂度的计算公式为：

$$f(a)=\log\frac{(a\otimes d)}{C(a,b)S} \tag{7}$$

式中：$f(a)$ 表示隐私数据信息 a 的明文复杂度，d 表示多项式的迭代次数，S 表示明文符号。

根据公式（7）的计算结果，本研究通过逼近数据信息的明文符号，计算其密文长度区间，其公式为：

$$\begin{cases}\min F(a,b)=f(\frac{a+b}{2})-\left|\frac{a-b}{2}\right|\\ \max F(a,b)=f(\frac{a+b}{2})+\left|\frac{a-b}{2}\right|\end{cases} \tag{8}$$

式中：F 表示隐私数据信息的密文长度。

通过公式（8）的分析计算，将计算所得的最大长度值及最小长度值作为隐私信息密文长度区间，将其设置为后续隐私加密的边界阈值。

1.3 阈值约束下添加密文实现隐私加密

根据上节所得的密文长度区间阈值约束，为数据库实训平台的数据信息添加隐私加密的密文，完成数据库实训平台信息隐私加密。

定义信息隐私加密的密文格式，其公式为：

$$G=\{K,E,D,A\} \tag{9}$$

式中：G 表示信息隐私加密的密文格式，K 表示密钥算法，E 表示密文的加密机制，D 表示解密算法，A 表示加密评估算法。

分别定义公式（9）中的 K、E、D、A 四个格式单元。设计数据库实训平台隐私信息加密的密钥算法，在原始的数据信息中随机选取两个等长的素数单元，两个素数单元之间的关系公式[9]为：

$$K=\begin{cases}\lambda(p,q)=(g+m)^2\\ l(p,q)=(p-1)(q-1)\end{cases} \tag{10}$$

式中：p 和 q 分别表示随机选取的两个素数单元，λ 表示两者的最大公约数，l 表示两者的最小公倍数，g 表示两个素数单元所对应的整数，m 表示复数。

根据该关系，基于上节公式（8）得到的密文长度区间，设计密钥算法所对应密文的加密机制，其公式为：

$$E=\frac{g^m\cdot r^K}{M},\min F(a,b)\le M\le\max F(a,b) \tag{11}$$

式中：r 表示随机数，M 表示根据信息明文长度给定的明文内容。

设计该密文机制对应的解密算法，其公式为：

$$D=\frac{\|E\|^y}{P\cdot r}W(i) \tag{12}$$

式中：P 表示解密向量，$W(i)$ 表示平台隐私数据信息的安全参数，y 表示密文与明文的互信息系数。

基于信息隐私加密的安全性需求，对加密密文进行自评估。设计加密评估算法公式[10]为：

$$A=\frac{Y(E+D)^{\sigma^2}}{Y(G)\otimes w} \tag{13}$$

式中：Y 表示密钥密文元组，σ 表示密文在信息架构中的分布概率，w 表示密文所对应的公钥。

将公式（10）~（13）获得的 K、E、D、A 代入公式（9），为数据库实训平台的隐私数据信息生成相应的密文，完成数据库实训平台信息隐私加密方法的设计过程。

2 实验

2.1 实验准备

为评估本研究提出的数据库实训平台信息隐私加密方法的实际应用可行性，设计了对比实验。通过对比实验测试结果，分析该方法在实践中的有效性。

本次实验全程于计算机中进行。基于实验目的，在计算机环境中模拟搭建依托于某高校的数据库实训平台实际应用环境。实验计算机环境如图3所示。

图3 实验场景环境

如图 3 所示，本次实验共配备有两台计算机设备，一台用于搭建数据库实训平台的计算机环境，一台用于模拟生成该平台的运行数据以及实验结果的处理分析。两台计算机设备的配置完全一致，具体的配置参数如表 1 所示。

表 1 实验计算机配置参数

序号	项目	配置参数
1	型号	ThinkServer 430
2	操作系统	Windows10
3	物理服务器操作系统	Ubuntu16.04 LTS
4	CPU	Intel(R) Core(TM) i7-10700 CPU
5	内存	64 GB DDR3
6	主频	2.90 GHz
7	组件	Horizon、Cinder、Nova-compute、Keystone、Glance
8	数据库场景	MySQL、Neo4j、Mongo
9	默认数据文件传输	Ansible
10	大整数库	NTL-v11.3.2

在如表 1 所示的计算机环境中，搭建实验所依托的数据库实训平台模拟架构。该平台架构为层次架构，如图 4 所示。根据图 4 所示的层次架构，在实验计算机环境中模拟搭建基于数据库实训平台。在计算机中设置 MySQL 和 MongoDB 进行数据库节点的单机部署，同时引入 Neo4j 作为非结构化数据库，构建数据库实训平台的核心架构。

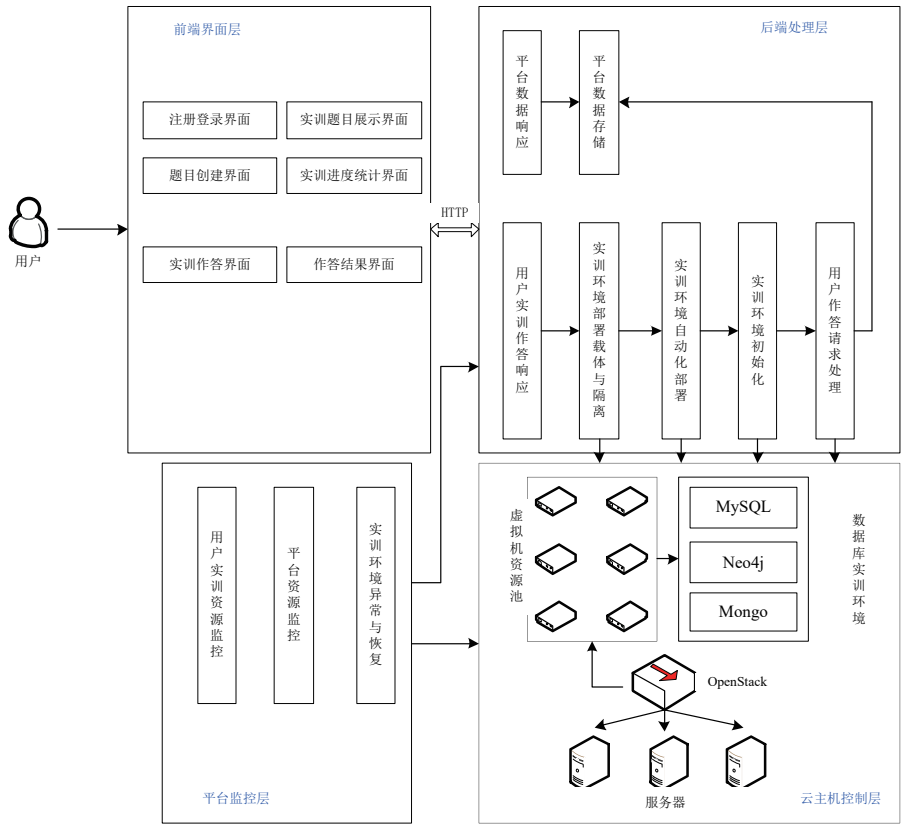

图 4 数据库实训平台层次架构

在完成数据库实训平台的模拟搭建后，在另一台配置好的实验计算机中模拟生成该平台的运行数据。在数据库实训平台的云主机控制层中，采用 mybatis3 实现平台数据信息的二次缓存单元，并根据该平台的核心性能，在后端处理层中使用 SpringMVC 实现平台数据算法的模拟运算逻辑。设置运算逻辑参数如下：Logistic 映射控制参数阈值设定为 4；混沌周期的解序列为 3；隐私信息的初始敏感值为 0.5；近似同态比较函数项式为 5；多项式的迭代次数为 100；平台隐私数据信息的安全参数为 0.6；密文与明文的互信息系数为 0.5；密文在信息架构中的分布概率为 0.3。基于这些数据运算逻辑，在另一台实验计算机中模拟生成平台数据信息加密区间，如表 2 所示。

表 2 数据库实训平台数据信息加密区间

数据信息类型	有符号值存储范围	无符号值存储范围	字节长度 /bit
TINYINT	-128 ~ 127	0 ~ 255	1
MEDIUMINT	-32 768 ~ 32 767	0 ~ 65 535	3
BIGINT	- 223 ~ 223 - 1	0 ~ 16 777 215	8
SMALLINT	-231 ~ 231 - 1	0 ~ 4.294 967E9	2
INT	-263 ~ 263 - 1	0 ~ 1.099 51E12	4

根据如表 2 所示的数据信息格式，模拟生成本次实验所需的数据库实训平台数据。在此基础上，根据该平台在实际应用中的基本需求，将模拟生成的数据信息划分为不同的整数类型，并在平台架构的后端处理层中，选择相应的存储格式。

对生成的平台数据信息进行明文处理，完成数据清洗及去重等预处理步骤。将处理好的数据整合成为本次实验的数据集，作为后续信息隐私加密的实验对象。完成上述工作准备后，启动本次数据库实训平台信息隐私加密实验。

2.2 实验结果分析

2.2.1 Logistic 映射下的隐私数据分类集成效果实验

在上述搭建的实验环境中开展该方法的应用测试，并根据实验结果分析本研究所提出方法的实践应用可行性。

在模拟生成的数据库实训平台数据信息集中，随机筛选部分数据信息作为测试本研究所提方法的实验数

据，测试本文方法隐私数据分类集成效果。该数据在实训平台存储架构中的原始分布态势如图 5 所示。

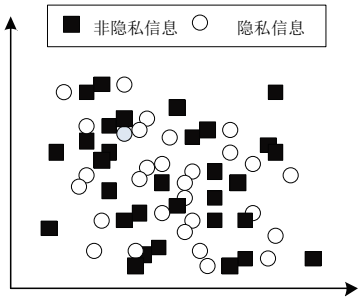

图 5 实训平台数据原始存储分布态势

在如图 5 所示的环境下，采用本研究所提方法对该平台数据信息进行分类集成处理，处理结果如图 6 所示。

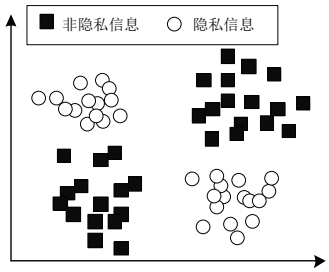

图 6 分类集成处理后数据库实训平台隐私信息分布

如图 6 所示，本研究提出的方法利用降维和 Logistic 映射将分布较为杂乱的多维度原始平台数据信息分类处理，形成界线分明的存储分布态势，更有利于后续加密。

2.2.2 数据库实训平台信息隐私加密效果实验

在此基础上，继续应用本研究所提方法、文献 [2] 方法、文献 [3] 方法对其进行信息隐私加密处理，得到结果如图 7 所示。

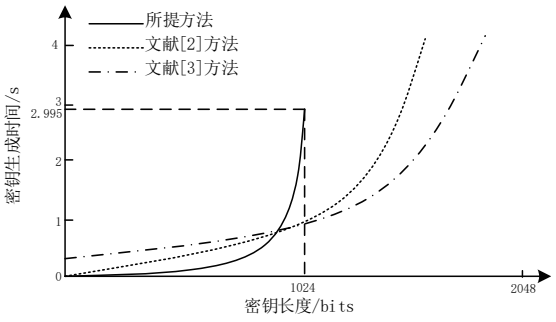

图 7 数据库实训平台信息隐私加密结果

根据图 7 可知，本研究针对该数据中不同信息的隐私程度，生成了相应长度的密钥。并且这些密钥的长度符合表 2 中设定的加密密文长度区间阈值。这些密钥的长度严格遵循了表 2 中设定的加密密文长度区间阈值。尽管密钥生成所需时间呈现指数级增长的态势，但总体加密时间仍然被有效地控制在 3 s 以内。与另外两种方法相比，本研究所提出的方法在密钥长度和生成时间方面都展现出了更高的合理性。主要原因在于本文方法使用近似同态比较分析计算隐私信息密文长度区间阈值，约束密文长度在合理范围内。通过这一步骤，本研究能够精确地确定密文长度的区间阈值，从而在加密过程中实现对密文长度的有效控制。这不仅避免了加密结果超出预期范围，减少了信息泄露的风险，还有助于提高加密效率，减少资源消耗。本研究所提出的方法在密钥长度和生成时间方面表现出更高的合理性。

2.2.3 数据库实训平台信息隐私加密效果量化

为了更加直观地体现出本次数据库实训平台信息隐私加密实验结果的有效性，设置一个定量指标来衡量不同信息隐私加密方法的实验结果。基于数据库实训平台在实践应用过程中对隐私数据信息的安全需求，将本次数据库实训平台信息隐私加密实验的定量评价指标设定为 Lyapunov 指数。根据该结果评价指标，分析不同隐私加密方法对数据库实训平台中数据信息的隐私加密情况。这一结果评价指标的计算公式为：

$$\Psi=\frac{1}{t_m-t_0}\sum_{t_m=1}^{N_m}\ln\frac{L_m}{L_0} \tag{14}$$

式中：Ψ 表示 Lyapunov 指数的结果评价指标计算值，t_m 表示信息隐私加密全过程所消耗的时间，t_0 表示加密明文生成所消耗的时间，N_m 表示该轮次实验中所包含数据库实训平台隐私信息的数据量，L_m 表示加密明文字节长度，L_0 表示隐私数据信息的字节长度。

基于公式（14）的计算结果，分析不同隐私加密方法在数据库实训平台信息隐私加密实践中的加密性能。计算所得的 Lyapunov 指数数值越大，则表明相应方法对实训平台数据隐私的初始条件越敏感，加密的复杂度则会相应地有所增高，加密结果的安全性也就越强。基于此，本次实验通过 Lyapunov 指数的结果评价指标，分析不同隐私加密方法的实践应用有效性。

为了保证本次实验结果的有效性，采用对比分析的方法对本次实验结果进行评价。分别采用文献 [2] 方法、文献 [3] 方法以及文献 [4] 方法作为本次实验的对比方法，将其分别命名为方法 1、方法 2 以及方法 3。基于上述设定的结果评价指标，分析并讨论不同方法的数据库实训平台信息隐私加密实验测试结果。

本次实验进行了多个轮次，每个轮次实验中，不同隐私加密方法所针对的数据库实训平台的隐私数据信息保持完全一致，以确保本次实验结果横向比较的有效性。经过实验，获得了不同方法在数据库实训平台信息隐私加密方面的实验结果，具体情况如图 8 所示。

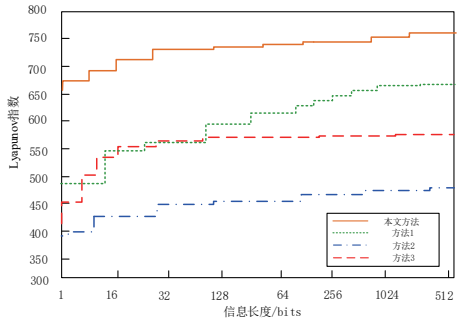

图 8 不同方法信息隐私加密 Lyapunov 指数对比

由图 8 可知，本次数据库实训平台信息隐私加密实验显示出，不同隐私加密方法的 Lyapunov 指数结果不同。方法 1 和方法 3 在原始信息长度在 128 bit 时，Lyapunov 指数呈现出类似的范围，均在 450 ~ 550 之间。然而，在后续的信息长度增加实验中，方法 1 的 Lyapunov 指数明显提高。相比之下，方法 2 在多个信息长度增加的实验轮次中，所表现出的 Lyapunov 指数相对较低，最低为 370，最高指数值仅为 435，与其他方法有着较大的差距。本研究所提方法在信息长度增加的多轮次实验中表现出了较高的 Lyapunov 指数，最低仅为 675，最高值能够达到 748，相比其他三种方法有着明显的提升。

从这一实验结果可知，本研究所提出的数据库实训平台信息隐私加密方法在实践应用中表现出了较为优质的加密结果，Lyapunov 指数始终较大，具备较高的实践应用有效性。主要原因在于使用近似同态比较分析计算隐私信息密文长度区间阈值，并约束密文长度在合理范围内。这一步骤确保了加密过程中密文长度的精确控制，避免了信息泄露的风险，并提高了加密的安全性。通过设定合理的密文长度区间阈值，本方法能够有效地限制密文长度的变化，从而确保加密结果的稳定性和可靠性。这种对密文长度的有效控制不仅提高了加密效率，还增强了数据的机密性和完整性。本研究所提出的数据库实训平台信息隐私加密方法在实践应用中表现出了较为优质的加密结果，并具备较高的实践应用有效性。

3 结语

数据库实训平台在教学培训以及软件开发运维等多个领域中均有着广泛应用。为了保障该平台在实际应用过程中的信息安全需求，本研究提出一种数据库实训平台信息隐私加密方法。特别是其中密文长度区间阈值的设定，展现出了显著的有效性。这一创新性的方法设计不仅满足了在数据库实训平台中对信息安全的严格要求，还通过精确控制密文长度，有效防范了信息泄露风险，显著提升了数据的安全性和完整性。实验结果表明，采用本研究所提方法加密后的信息，其 Lyapunov 指数始终保持在较高水平，充分证明了该方法在隐私保护方面的卓越性能。然而，本研究所提方法由于各种各样的因素，难免存在一些问题。由于条件有限，本研究在数据库实训平台信息的语义扩展方面尚未深入探索，信息间的语义关联仍有待进一步明确。在未来的工作中，将致力于研究平台信息在语义搜索和语料库关键词数量扩充方面的隐私加密方法，以期实现更加精细和严谨的信息安全保护，推动数据库实训平台的持续发展与广泛应用。

参考文献：

[1] 熊爱明，李明倩，刘芳．基于混沌映射的数据库信息隐私加密储存算法 [J]. 吉林大学学报 (信息科学版), 2023, 41(3): 459-464.

[2] 宋永占，奚磊，崔巍，等．基于隐藏分类算法的电网隐私数据多层级加密研究 [J]. 微型电脑应用 ,2023,39(11):60-64+68.

[3] 姜春峰．基于属性分类的分布式大数据隐私保护加密控制模型设计 [J]. 计算机测量与控制 ,2023,31 (11):221-227.

[4]GHOSAL S K, MUKHOPADHYAY S, HOSSAIN S,et al.Application of Lah transform for security and privacy of data through information hiding in telecommunication[J].Transactions on emerging telecommunications technologies, 2020, 32(2): 7-9.

[5]YAO Y, WANG Z.Privacy information antistealing control method of medical system based on cloud computing[J].International journal of communication systems,2020,35(5):1-12.

[6] 侯欣怡，刘晋璐，张茜，等．多数据所有者场景下具有访问模式和搜索模式隐私的对称可搜索加密方案 [J]. 密码学报 , 2023, 10(6):1241-1265.

[7] 冯涛，陈李秋，方君丽，等．基于本地化差分隐私和属性基可搜索加密的区块链数据共享方案 [J]. 通信学报 , 2023, 44(5): 224-233.

[8] 冯云霞，王西贤．基于椭圆曲线加密算法的工业物联网数据隐私保护方案 [J]. 智能计算机与应用 ,2022,12(12):110-113+121.

[9] 孙晓妮，廖春艳．体医融合背景下高等体职院校搭建运动营养与康复实训平台的运行保障机制研究 [J]. 当代体育科技 , 2023, 13(4):33-36.

[10] 江元，李晓明，尚云飞．基于混沌序列的电力营销数据去隐私化加密方法研究 [J]. 微型电脑应用 ,2022,38(2):109-112+115.

【作者简介】

付思思（1993—），女，江西南昌人，硕士研究生，讲师，研究方向：图像处理、人工智能。

（收稿日期：2024-02-20）