doi: 10.7690/bgzdh.2026.05.005

基于多层感知学习的档案隐私信息加密存储系统设计

王　颖
（保定市交通运输综合行政执法支队，河北 保定 071000）

摘要：为提升数字档案信息数据的安全，设计基于多层感知学习的档案隐私信息加密存储系统。明确系统的建立要求，构建数字档案隐私信息加密存储系统整体框架设计；对框架中数据认证、检索、管理等硬件模块展开具体的功能分析；通过系统对数字档案隐私信息数据加密、解密等软件的流程设计，并通过多层感知学习器对系统数据实施噪声去除处理，实现档案隐私信息的加密存储。实验结果表明：使用该系统开展数字档案隐私信息加密储存时，数据的丢失率低、加密时间短、加密储存效果好。

关键词：数字档案；隐私信息；加密存储；多层感知学习；系统设计
中图分类号：TP309　　**文献标志码：**A

Design of Archival Privacy Information Encryption Storage System Based on Multi-layer Perception Learning

Wang Ying
(*Baoding Municipal Transportation Comprehensive Administrative Law Enforcement Detachment*, *Baoding* 071000, *China*)

Abstract: In order to improve the security of digital archival information data, an archival privacy information encryption storage system based on multi-layer perception learning is designed. Make clear the requirements of the system, construct the overall framework design of the digital archives privacy information encryption storage system, and analyze the specific functions of the hardware modules such as data authentication, retrieval and management in the framework; Through the process design of encryption and decryption software of digital archives privacy information data, and through the noise removal of system data by multi-layer perception learning device, the encryption and storage of archives privacy information is realized. The experimental results show that the data loss rate is low, the encryption time is short, and the encryption storage effect is good when the system is used to encrypt and store the privacy information of digital archives.

Keywords: digital archives; private information; encrypted storage; multi-layer perception learning; system design

0　引言

随着信息化时代的到来，信息数据量增长迅速，信息数据存储管理[1]变得愈加困难。依据国家有关部门调查结果，截至 2019 年，我国互联网用户规模已经超出 13 亿，是全球网络用户的三分之一。信息时代背景下，大量的企业、个人将互联网技术应用到日常工作中，数字化档案至此应运而生。由于数字化档案中存在大量的敏感数据信息，若敏感信息泄露会直接威胁企业甚至国家的财产安全；因此，对数字化档案[2]开展加密存储，避免信息泄露，成为当前学者积极讨论的话题之一。

文献[3]提出面向云存储的数据加密系统与技术研究。依据 JavaScript 程序分析方法对数据开展识别分配处理，依据处理结果完成敏感数据的加密；再依据网关的密文搜索功能，从而最大限度地实现加密数据的保护、存储。该方法由于未能使用多层感知学习技术滤除数据噪声，所以其在数据加密储存时，执行时间长。

文献[4]提出面向医疗数据安全存储的增强混合加密方法。首先对数据的储存风险开展详细的分析，依据分析结果提出基于数据安全存储的信息加密存储算法；再引入非对称加密方法对数据加密存储算法实施优化处理；最后通过优化后的数据加密存储算法实现数据的安全加密存储。该方法由于在数据加密时存在问题，所以其数据加密储存效果差。

文献[5]结合可撤销属性加密和快速密度聚类 2 种方法，对非结构化大数据安全存储系统展开设计：首先，提高属性撤销方法对数据进行撤销处理，根据预处理结果，建立数据的安全储存结构；其次，基于数据攻击类型的辨识结果对数据攻击行为展开规避，同时采用霍夫曼压缩方法压缩处理数据，从

收稿日期：2024-12-04；**修回日期：**2025-01-05
第一作者：王　颖(1984—)，女，内蒙古人。

而有效地实现数据的安全加密存储。该方法由于在属性撤销时存在问题，所以其在数据加密储存时，数据压缩效果差。

为解决上述数据信息加密存储方法中存在的问题，提出基于多层感知学习的档案隐私信息加密存储系统。

1 档案隐私信息加密存储系统整体设计

1.1 系统设计基本要求

由于设计档案隐私信息加密存储系统[6]的目的是为保证档案隐私信息的安全，辅助管理人员完成数字化档案的基本管理，所以档案隐私信息加密存储系统在设计时，需满足如下要求：

1) 安全认证。建立档案隐私信息加密存储系统时，档案隐私数据能够安全加密，是整个系统建立的关键，系统建立时，除了保证档案信息数据的安全加密[7]，还要保证加密数据能够在安全环境中存储、输出；设计客户端控制模块、服务器控制模块以及用户注册登录模块 3 部分。

2) 安全检索。系统建立时，除了保证档案信息数据的安全加密[7]，还要保证数据在检索过程中能够准确、有效地进行检索；设计服务器检索模块与客户端检索模块。

3) 安全管理。安全管理是为有效保障数字档案信息的安全。主要运用用户管理、云服务管理以及明文存储管理、密文储存管理 4 个方法和手段。分析和研究各种不安全因素，从技术、组织和管理方面采取有力的措施，解决和消除各种不安全因素，防止事故的发生。

4) 安全储存。数据库的建立是安全储存中重要的一部分，是整个安全储存的关键；因此，在档案隐私信息加密存储系统时，需合理开发建设数据库，从而保证档案隐私信息的安全加密存储。

5) 安全传输。数字档案信息泄露会直接影响国家、企业的财产安全；因此，使数据安全保密地进行传输，是极其重要的，防止数据传输时被截获。

1.2 档案隐私信息加密存储系统整体框架设计

依据上述系统建立要求，完成档案隐私信息加密存储系统的整体框架设计，具体如图 1 所示。

依据建立的整体框架可知：档案隐私信息加密存储系统由认证模块、传输模块、检索模块、管理模块、存储模块组成，通过模块之间的配合，实现档案隐私信息的加密存储。

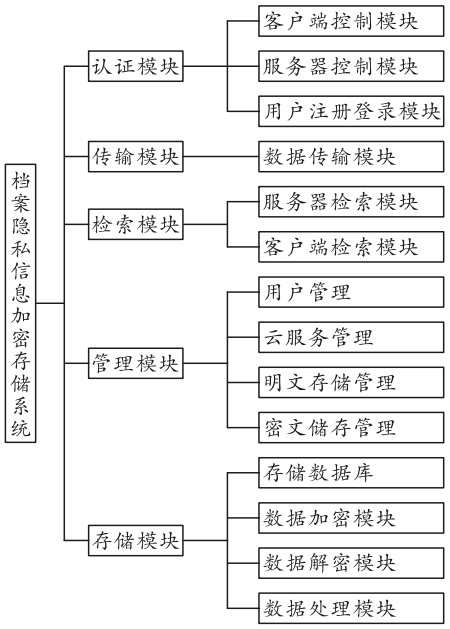

图 1 档案隐私信息加密存储系统整体框架

1.3 系统硬件模块分析

1.3.1 认证模块

该模块分成客户端控制、服务器控制以及用户注册登录 3 部分，主要负责加密信息的安全认证。

在用户注册登录子模块中，新用户注册后，在用户端构建数据库，并将该数据库与系统总数据库连接，从而保证数据的实时传输[8]。

客户端控制模块主要负责控制用户在系统中开展档案隐私数据上传、下载、删除等任务操作，在提高用户体验的同时，保证系统内数据的安全。

服务器控制模块主要负责存储控制用户档案的各项隐私敏感数据，当用户需要使用隐私数据时，利用服务器中缓存的密钥对隐私数据解密处理，再通过数据的明文形式，将信息发送给用户。

1.3.2 检索模块

该模块主要负责管理者检索相关信息。管理人员在系统登录后，输入检索关键词，系统数据库会在接收指令后将管理者需要的数据密文发送给管理者，管理者通过密码解锁密文，完成数据信息的获取。

1.3.3 管理模块

系统管理模块是整个系统的核心，整个模块包含用户管理、云服务管理、明文存储、密文储存 4 个子模块。

构建档案隐私信息加密存储系统时，系统用户一般设置成系统管理人员以及普通用户 2 种，系统管理人员具备操作系统的所有权限，普通用户只

具备云服务管理、明文存储以及密文储存等操作权限。

用户管理模块主要负责档案信息的添加、修改以及查询功能；云服务管理主要对接数据信息存储模块，主要负责对存储数据信息添加、查询等任务，只对系统管理员开放；明文存储管理主要是负责将档案半公开信息打包以文件形式储存到存储模块中；密文存储管理负责将档案隐私信息加密处理，加密完成后将密码发送给管理员，并将加密信息存储到数据库中，完成数据的加密存储。

1.3.4　储存模块

系统储存模块主要负责档案各项数据的储存。该模块选用存储数据为系统主要数据库，以便档案信息的输入和输出。数据储存模块主要负责数据加密、解密以及数据的处理。

数据加密、解密模块主要负责档案隐私信息数据的加密、解密。数据一经加密，数据长度发生变化，这时就需要通过二进制文件存储密文字节，解密时，密文需要密码结合存储的字节，实现数据的验证，完成解密。

数据处理模块主要负责档案隐私数据以及系统数据的处理工作。

1.3.5　传输模块

传输模块主要负责档案隐私数据的往来传输，包括向内外部系统间的数据库进行数据传输，以便与用户基于数据传输模块建立连接，当接收到用户发送的数据传输请求时，根据所述数据传输请求将档案隐私数据从数据库中获取并发送给用户。

2　软件设计

档案隐私信息加密存储系统的软件设计主要分成档案隐私信息传输、档案隐私数据加密、档案隐私数据解密以及系统整体加密存储流程 4 部分。

2.1　档案隐私信息加密储存系统数据处理流程

系统的数据处理流程如图 2 所示。

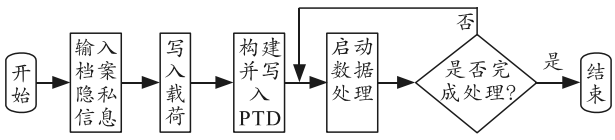

图 2　档案隐私信息加密储存系统信息处理流程

2.2　档案隐私信息数据传输流程

档案隐私信息数据传输模块软件实现流程如图 3 所示。

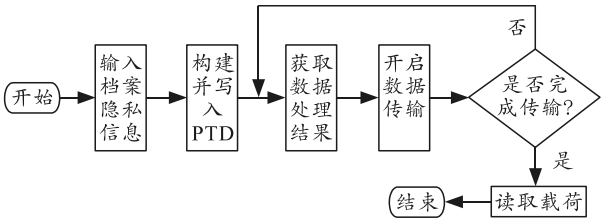

图 3　档案隐私信息数据传输模块软件实现流程

档案隐私信息加密存储系统数据传输模块通过数据的处理结果开启传输，通过建立的 PTD 对整个传输流程实施监控，规避传输流程中档案隐私敏感信息的安全。由于系统运行时，会出现大量的噪声数据，当噪声数据过多就会降低后续数据传输与存储的准确性，所以在处理过程中需采用多层感知学习器[9]对系统数据实施噪声去除处理。

将滤波算法引入多层感知学习器中，把系统数据权值看作系统状态变量，利用多层感知学习器构建去噪模型：

$$\left.\begin{aligned} e_j &= e_{j-1} + s_j \\ u_j &= h(e_j,\ \boldsymbol{y}_j) + c_j \end{aligned}\right\}。\tag{1}$$

式中：u_j 为多层感知学习器模型输出量；$\boldsymbol{y}_j$ 为输入向量；e_j 为模型权值；$h(e_j, y_j)$为多层感知学习器激活函数；s_j 为系统的过程噪声；c_j 为高斯噪声。

档案隐私数据加密存储系统的噪声去除[10]：

1) 初始化系统，建立系统先验密度函数 $q(u_j|u_{1,j-1}, P_j)$完成系统数据噪声估计：

$$q\left(P_j \mid u_{1,j}\right) = \frac{q(u_j \mid u_{1,j-1}, P_j)}{q(u_j \mid u_{1,j-1})} q\left(P_j \mid u_{1,j-1}\right)。\tag{2}$$

式中：$q(P_j|u_{1,j})$为系统的噪声估计值；$\boldsymbol{j}$ 为系统当前状态向量；P_j 为系统噪声。

2) 依据计算出的噪声估计值[11]，建立系统噪声协方差矩阵，结合系统的数据重要性采样，计算数据的正态分布值。

3) 对计算结果归一化处理，获取模型输出，实现系统数据的噪声滤除。

2.3　档案隐私信息密钥生成流程

档案隐私信息密钥[12]生成流程如图 4 所示。

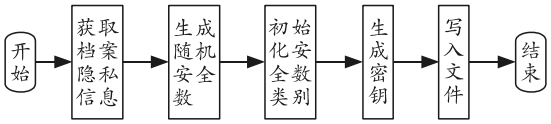

图 4　档案隐私信息密钥生成流程

2.4　数据加密、解密流程

档案隐私数据的加密、解密[13]流程如图 5—6 所示。

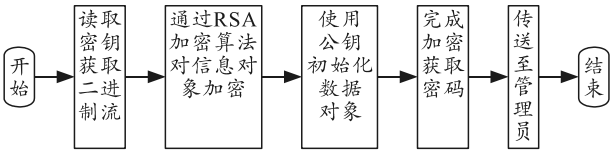

图 5　档案信息加密流程

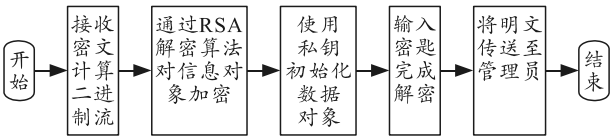

图 6　档案信息解密流程

生成 2 个任意不同的大质数 p、q。

由 2 个大质数 p、q 相乘得到：$n=p\times q$；

欧拉函数 $f(n)=(p-1)\times(q-1)$。

设 d 与 $f(n)$互质，$d\in(1,f(n))$，找到任意一个大整数 e 使得 $d\times e$ 除$(p-1)\times(q-1)$的余数为 1。

(n, d)构成公钥，C 为密文，M 为明文，加密 $C=M^{d \bmod n}$。

(n, e)构成私钥，C 为密文，M 为明文，解密 $M=C^{e \bmod n}$

依据上述过程完成信息数据加密后，数据会以密文的形式储存在存储数据库内，当数据库接收到指令后，会将密文发送给用户，用户通过检索验证获取密码，结合解密算法实现数据的解密。

2.5　数据存储流程

档案隐私信息加密存储[14-15]流程如图 7 所示。

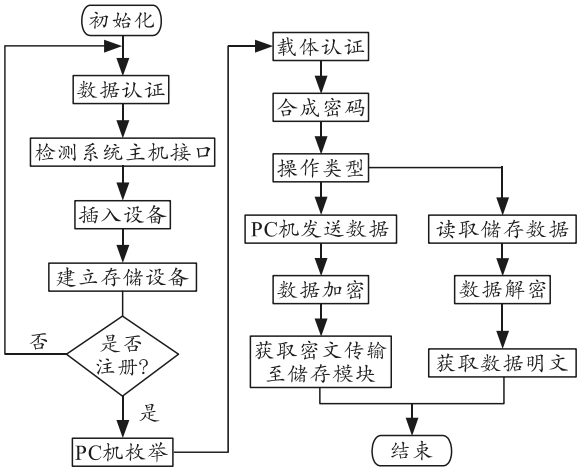

图 7　档案隐私信息加密存储流程

最后依据设计的软件实现流程完成档案隐私数据的安全加密存储。

3　实验

分别采用基于多层感知学习的档案隐私信息加密存储系统(笔者所提方法)、面向云存储的数据加密系统与技术研究(文献[3]方法)、面向医疗数据安全存储的增强混合加密方法(文献[4]方法)展开测试。

选取信息丢失率、数据压缩效率以及时间开销效率作为数据加密储存方法的测试指标，测试所提方法、文献[3]方法以及文献[4]方法在数据加密存储过程中的效果。

1) 信息丢失率测试。数据在开展安全加密存储时，可通过导入文件信噪比大小以及信息损失百分比测试加密存储方法的信息丢失情况，结果如图 8—9 所示。

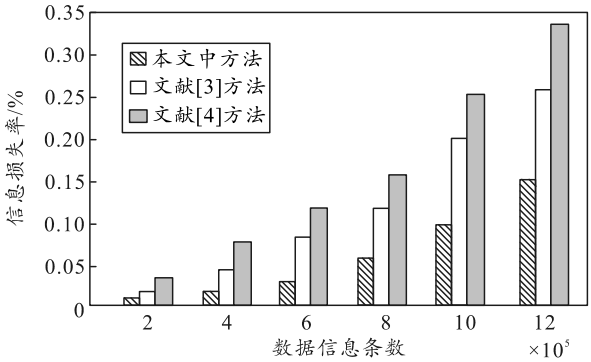

图 8　不同方法的信息损失百分比测试结果

分析图 8 可知，随着数据量的增加，3 种方法检测结果均会随之增长。其中，笔者所提方法在数据加密存储时检测出的信息数据损失百分比低于文献[3]以及文献[4]方法。

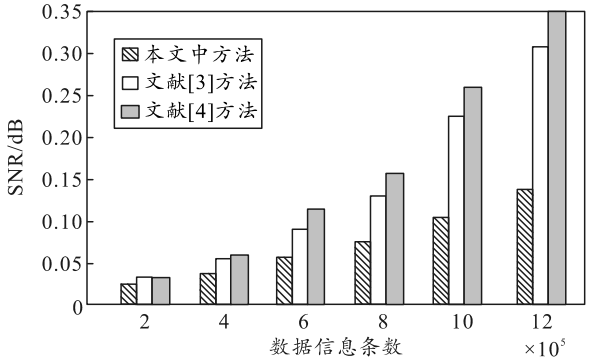

图 9　不同方法文件导入信噪比测试结果

开展数据加密存储时，数据导入时的信噪比越低，说明数据在加密储存时的信息丢失率越小，反之则越大。依据图 9 可知，随着检测信息数据的增加，3 种方法检测出的信噪比均出现了不同程度的上升。但笔者所提方法的检测结果是 3 种方法中最小的，说明其在开展数据加密存储时具备有效性。

2) 数据压缩效率测试。选取数据加密储存时的压缩比为数据压缩效率测试指标，笔者所提方法、文献[3]方法以及文献[4]方法的数据压缩效率，结果如图 10 所示。

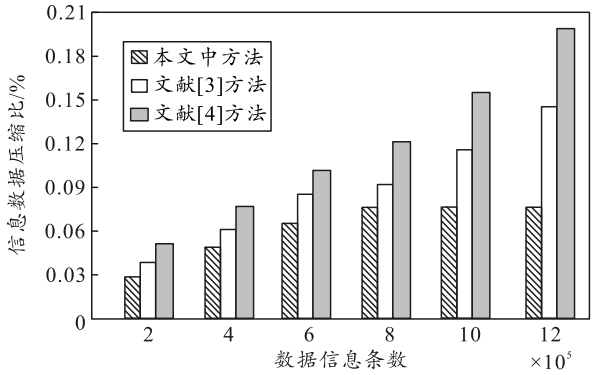

图 10　不同方法的信息数据压缩比测试结果

数据加密储存时，数据压缩比越高，说明储存方法的储存效果越差，反之则越高。分析图 10 可知：笔者所提方法检测出的数据压缩比优于其他 2 种方法的检测结果，这主要是因为所提方法在数据加密储存前，使用多层感知学习器对数据噪声实施了滤除处理；因此，该方法在数据加密储存时，数据的安全压缩效率越好。

3) 执行时间测试。利用笔者所提方法、文献[3]方法以及文献[4]方法开展数据加密储存时，测试 3 种方法的数据加密储存执行时间，测试结果如表 1 所示。

表 1　不同方法的加密储存执行时间测试结果　　s

数据条数	所提方法	文献[3]方法	文献[4]方法
10×10^4	0.02	0.06	0.08
20×10^4	0.15	0.19	0.50
30×10^4	0.39	0.42	1.29
40×10^4	0.77	0.98	2.84
50×10^4	1.25	1.55	4.69
60×10^4	2.21	2.71	6.25
70×10^4	3.85	4.29	8.99
80×10^4	4.63	5.37	10.23

分析表 1 可知：笔者所提方法在开展数据加密储存时，检测出的数据加密储存时间是 3 种方法中最低的。由此可证明，该方法在数据加密储存时，加密存储时间短、加密储存效果好。

4　结束语

随着档案数字化的不断进步，数据档案隐私信息的加密储存变得尤为重要。针对传统数据加密储存方法中存在的问题，提出多层感知学习的档案隐私信息加密存储系统设计方法。通过系统的建立要求，完成整个系统的整体框架设计；对系统硬件开展详细的功能分析；通过软件的流程设计，实现数据的安全加密储存。该系统在设计检索模块时，还存在些许问题，今后会针对该项缺陷继续优化。

参考文献：

[1] 邵波, 单轸, 王怡. 新一代服务平台环境下的智慧图书馆建设: 业务重组与数据管理[J]. 中国图书馆学报, 2020, 46(2): 27-37.

[2] 黄国彬, 闫鑫. 美国高校面向个人数字存档信息的管理规范研究[J]. 图书情报工作, 2021, 65(4): 123-134.

[3] 韩培义, 刘川意, 王佳慧, 等. 面向云存储的数据加密系统与技术研究[J]. 通信学报, 2020, 41(8): 55-65.

[4] 康海燕, 邓婕. 面向医疗数据安全存储的增强混合加密方法[J]. 北京理工大学学报, 2021, 41(10): 1058-1068.

[5] 谷保平, 马建红. 可撤销属性加密结合快速密度聚类算法的非结构化大数据安全存储方法[J]. 计算机应用与软件, 2021, 38(5): 337-343.

[6] 张新文, 刘愉强, 刘同木, 等. 基于混合加密的浮标数据安全管理系统研究[J]. 热带海洋学报, 2020, 39(5): 117-123.

[7] 宋秀丽, 周道洋, 文爱君. d 维(t, n)门限量子同态加密算法的设计与仿真[J]. 电子学报, 2020, 48(5): 846-853.

[8] 方如举, 葛瑜, 孙伟, 等. 基于 WSNs 的智能配电网通信数据传输带宽的优化分配策略[J]. 电力系统保护与控制, 2021, 49(23): 88-95.

[9] 单德山, 张潇, 顾晓宇, 等. 基于多层感知深度学习的大跨度斜拉桥索力调整[J]. 桥梁建设, 2021, 51(1): 14-20.

[10] 崔少华, 李素文, 汪徐德. BP 神经网络和 SVD 算法联合的地震数据去噪方法[J]. 电子测量与仪器学报, 2020, 34(2): 12-19.

[11] 章硕, 孙斌, 李树涛, 等. 空间与光谱维度的高光谱图像噪声估计[J]. 遥感学报, 2021, 25(5): 1108-1123.

[12] 王立辉, 闫守礼, 李清. 一种轻量级数据加密标准循环掩码实现方案[J]. 电子与信息学报, 2020, 42(8): 1828-1835.

[13] 拜亚萌, 张燕玲, 邓小鸿. 自适应分块的医学图像混沌加解密算法[J]. 计算机应用研究, 2020, 37(5): 1478-1481.

[14] 赵越, 余红英, 王一奇. 一种高速数据存储方法的设计与验证[J]. 数据采集与处理, 2021, 36(2): 384-390.

[15] 罗伟, 饶冰, 蒋破荒, 等. 基于 X86 的分布式存储的数据库平台架构[J]. 控制工程, 2020, 27(2): 303-308.