doi：10. 12068/j. issn. 1005－3026. 2026. 20260032

多源异构数据的混沌融合加密方案

朱志良[1,2,3]，邢 萌[1]，于 海[1,2,3]，张 伟[1]
（1. 东北大学 软件学院，辽宁 沈阳 110169；2. 东北大学 工业智能与系统优化国家级前沿科学中心，辽宁 沈阳 110819；3. 东北大学 智能工业数据解析与优化教育部重点实验室，辽宁 沈阳 110819）

摘 要：针对物联网中多源异构数据的隐私保护问题，提出了1种基于分段线性混沌映射的多源异构数据安全框架. 与现有的主要针对单一类型数据或独立处理异构数据的方案不同，所提方案首先根据多源异构数据的内在固有特征，设计相应的数据提取策略，将其充分融合后抽象为统一的表现模式. 在此基础上，为保证多源异构数据的安全性，首先设计了1种双重块级置乱策略和1种基于比特级的低频系数加密算法，利用加密后的低频系数确定唯一值，作为非零高频系数扩散的起始位置，然后对存在的非零高频系数进行双向背离扩散操作，进一步加强了对高频信息的保护. 实验结果表明，该算法保障了多源异构数据的安全性，可以部署于标准计算机.

关 键 词：多源异构数据；隐私保护；分段线性混沌映射；块级置乱；双向背离扩散
中图分类号：TP 309.7 **文献标志码**：A **文章编号**：1005-3026(2026)07-0009-11

Chaos-Fusion Encryption Scheme for Multi-source Heterogeneous Data

ZHU Zhi-liang[1,2,3], *XING Meng*[1], *YU Hai*[1,2,3], *ZHANG Wei*[1]
(1. School of Software, Northeastern University, Shenyang 110169, China; 2. National Frontiers Science Center for Industrial Intelligence and Systems Optimization, Northeastern University, Shenyang 110819, China; 3. Key Laboratory of Data Analytics and Optimization for Smart Industry, Ministry of Education, Northeastern University, Shenyang 110819, China. Corresponding author: YU Hai, E-mail: yuhai@mail.neu.edu.cn)

Abstract: To address the privacy protection problem of multi-source heterogeneous data in the Internet of Things, a secure framework for multi-source heterogeneous data based on a piecewise linear chaotic map was proposed. Different from existing schemes that primarily focus on single-type data or handle heterogeneous data independently, in the proposed method, corresponding data extraction strategies were first designed according to the inherent characteristics of multi-source heterogeneous data to fully fuse them and abstract them into a unified representation mode. On this basis, to ensure the security of multi-source heterogeneous data, a dual block-level permutation strategy and a bit-level low-frequency coefficient encryption algorithm were first designed. The encrypted low-frequency coefficients were used to determine a unique value as the starting position for the diffusion of non-zero high-frequency coefficients. Then, a bidirectional deviation diffusion operation was performed on the existing non-zero high-frequency coefficients to further strengthen the protection of high-frequency information. The experimental results indicate that the proposed algorithm ensures the security of multi-source heterogeneous data and can be deployed on standard computers.

Key words: multi-source heterogeneous data; privacy protection; piecewise linear chaotic map; block-level permutation; bidirectional deviation diffusion

多源异构数据是在模式、系统、语义等方面存在差异的信息表达形态，在各个领域具有广泛

收稿日期：2026-03-22
基金项目：国家自然科学基金资助项目(61977014)；高等学校学科创新引智计划项目(B16009).
作者简介：朱志良(1962—)，男，辽宁沈阳人，东北大学教授，博士生导师.
通信作者：于 海，E-mail：yuhai@mail.neu.edu.cn.

的应用潜力和价值[1-4].在新兴的感知学习领域中,采用软硬件相结合的方式,通过“软件定义内核需求,硬件驱动机器实体”实现真正意义上的人机交互,包括机器人、智能家居、自动驾驶等.在此过程中,需要通过大量多源异构数据作为输入以支撑其感知、决策与操控的闭环,其底层核心逻辑即为多源异构数据的识别、转化、融合、重组等[5-6].此外,随着互联网的兴起,大量多源异构数据的产生给软硬件存储系统造成了巨大的压力,使得二者长期处于“供不应求”状态.与此同时,这些数据在传输过程中面临数据泄露、丢失、拦截、篡改、破坏等安全性问题[7-8].

基于Matthews[9]提出的利用混沌动力学原理构造加密算法的构想,Fridrich[10]于1997年提出了至今在数据安全领域广为应用的“置乱-扩散”框架.基于此框架,研究人员面向多元化载体提出了许多新型加密算法[11-17].Tang等[11]提出了1种基于Logistic映射和杂交链式反应的信息加密方案.通过杂交不同类型的发夹DNA(deoxyribonucleic acid)链,最终形成双链DNA聚合物,提高了DNA编码的随机性.由于DNA编码会引入大量的时间消耗,可能造成加密算法无法满足实时系统的高响应需求,Zhu等[12]设计了1种基于组合混沌系统的轻量级分组加密算法.实验结果表明,该算法不仅提升了加密效率,而且具有良好的可扩展性.相比文本,可视化图像被定义为携带大量信息且更受用户青睐的目标载体之一.为保障图像中信息的安全性,Wu等[13]提出了1种基于DNA和多个改进的一维混沌系统的图像加密算法.为了解决DNA编码类型数量受限的问题,Yu等[14]提出了1种新的基于DNA三倍体突变和超混沌系统的图像加密算法.而Signing等[15]结合Jerk混沌系统和DNA编码,设计了1种应用于文本和图像的加密系统.以上提出的加密算法并不适用于密度极大的音频数据.文献[16]提出了1种在MPEG(moving picture experts group)压缩背景下基于混沌和小波变换的音频加密算法,在时域-小波域-时域分别进行3次音频信号的置乱和扩散操作以保障音频信号的安全性.文献[7]首先利用正弦函数、幂函数、简单的运算等构建1个n维离散超混沌系统,通过1次一密的手段设计了新的音频加密方案.Zhao等[17]则根据用户多样化需求设计了1种支持差分解密的音频保护方案.

上述加密方案的设计均只针对单一信息源而设计,忽略了物联网(Internet of Things,IoT)中多源异构数据的多样化需求.此外,现有方案通常对异构数据进行独立处理[11-17],缺乏在不同数据模式之间进行互操作和扩展.为此,本文提出1种不同于现有数据加密方案的多源异构数据安全框架,以物联网中多源异构数据为研究载体,引入1种统一且灵活的处理模式.在这种模式下,多源异构数据并非孤立地进行处理,而是根据其内在结构和统计特征进行自适应转换与融合.具体地,该算法的设计结合具有高随机性、初值高敏感性、硬件友好性等特点的分段线性混沌映射[18],构建1种简单、高效的轻量化安全机制.首先,该机制能够有效适配多源异构数据的差异化特征.例如,对于图像和视频数据,可以在变换域进行结构化表示;对于音频数据,可以通过频域特征进行建模;而对于文本数据,则可以转化为符号序列或编码向量进行统一处理.此外,不同类型的数据通过柔性化映射被嵌入到统一的表示空间,从而实现跨模态的一致性加密处理,同时避免对各类数据固有结构的破坏.该方案在实现多源异构数据统一安全保护的同时,兼顾了数据特征保持、系统灵活性以及实际部署需求,为物联网场景下的异构数据安全提供了1种可行且高效的解决方案.

1 算法描述

针对单一信息源难以满足互联网用户个性化、多样化需求等现实问题,本文以多源异构数据为研究对象,深入分析其内在特征,并结合混沌安全算法,提出1种轻量级、高安全性的加密算法.该算法的整体流程图如图1所示,主要包含数据预处理、数据融合、格式一致化以及数据加密四部分.在数据加密部分,利用经典的“置乱-扩散”模型,分别对抽象出的多源异构数据进行重排与替换操作,以此保障数据的安全性.

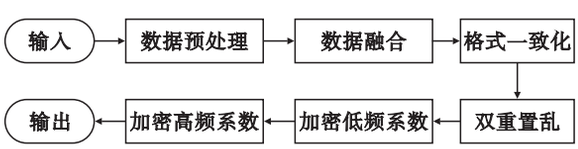


图1 算法整体流程图

Fig. 1 Overall flowchart of algorithm

1.1 数据提取与转换

本节主要描述多源异构数据的提取与转换,该过程在数据转换层中实现,如图2所示.分别以

文本、图像、音频、视频等作为目标载体，分析不同类型数据的固有特征并从多源异构数据中提取完整的数据，进而为后续数据融合层中数据的有效融合做准备.

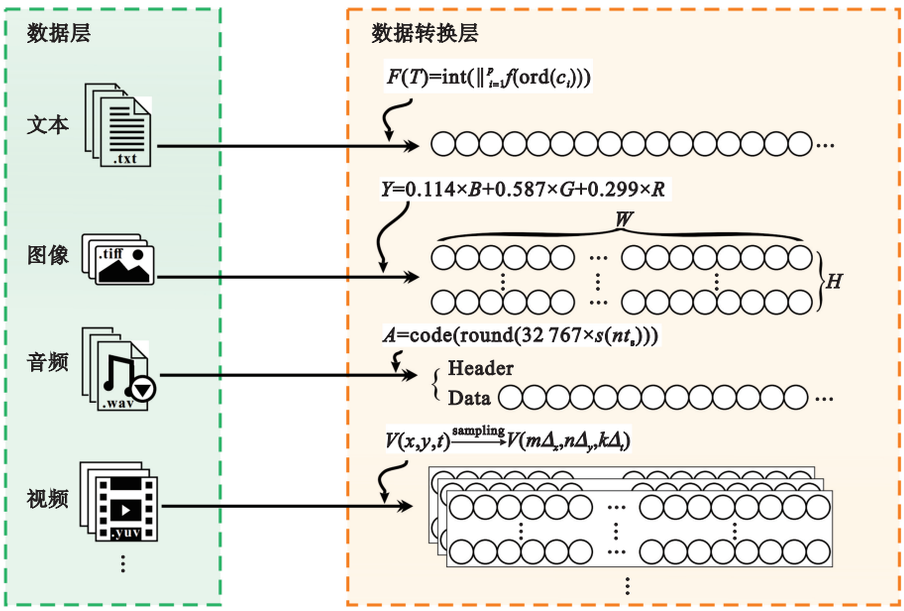


图 2　数据的提取与转换示意图

Fig. 2　Schematic diagram of data extraction and transformation

现有的文本主要表现形式分为 3 类：英文文本、中文文本及混合文本. 在不考虑词意、语序等问题的情况下，通常认为文本仅是 1 个由词构成的集合. 在本文中，文本数据首先进入数据转换层，读取原始的文本数据后，利用 UTF（unicode transformation format）-8 编码方式，将原始数据转换为计算机可识别的字节，转换公式如式（1）所示：

$$H(T)=\mathrm{int}(\|_{i=1}^{\theta}f(\mathrm{ord}(c_i))). \tag{1}$$

式中：$H(T)$ 表示转换后的数据；θ 表示文本数据的最大个数；c_i 表示第 i 个文本字符；ord(·) 表示 UTF-8 编码函数；$f(\cdot)$ 表示列表转换函数；$\|_{i=1}^{p}$ 表示拼接函数；int(·) 表示整数转换函数.

图像是以像素为单位的非结构化信息的常用表达方式之一. 现有的图像表现为非压缩图像和压缩图像 2 种类型，2 类图像针对的应用需求各不相同. 非压缩图像常被用于对细节信息要求较高的场景，如医疗影像、航天航空、高清监控等；压缩图像则以牺牲少量细节信息为代价，生成肉眼难以察觉的、关键信息完整的弱差异化图像. 考虑到现实成本问题，本文以压缩图像为主要研究对象. 数据转换层首先对原始图像进行预处理，即采用式（2）转换原始图像的格式（RGB（red green blue）转换为 YCbCr）.

$$Y=0.114\times B+0.587\times G+0.299\times R. \tag{2}$$

式中：R, G, B 分别表示原始输入图像在三通道中的像素值；Y 表示亮度值.

与上述两类可视化数据不同，音频数据是一种非结构化的听觉感知传导数据，且一段完整的音频数据中一般包含大量冗余信号，其占比约为 30%. 目前常见的音频存储格式为 wav，FLAC，MP3 等. 音频数据通过数据转换层，原始音频文件中的模拟信息被转换为数字信息，转换公式如式（3）所示：

$$A=\mathrm{code}\left(\mathrm{round}\left(32\,767\times s\left(nt_s\right)\right)\right). \tag{3}$$

式中：A 表示转换后的音频数据序列；t_s 表示音频采样周期；n 表示采样点；$s(nt_s)$ 表示在 nt_s 时的采样值；round(·) 表示四舍五入函数；code(·) 表示脉冲编码调制算法.

可视化视频数据通常可视为由若干图像序列与音频信息构成的多元数据. 视频数据通常以帧作为基本单位，并按照时间顺序排列形成连续的动态视觉序列. 在完整的视频数据中，空间域和时间域均存在大量冗余信息. 为提高压缩效率，主流视频编码标准（如 H.264/AVC，H.265/HEVC 等）通过预测、变换、滤波以及熵编码等技术对视频信号进行压缩，从而有效降低视频数据的存储和传输开销. 在视频采集过程中，连续的视频信号通过空域与时域上的离散采样，被转换为计算机可处理的数字视频数据，计算公式如式

(4)所示:

$$V(x,\ y,\ t)=V(m\Delta_x,\ n\Delta_y,\ k\Delta_t). \tag{4}$$

式中:$V(x,y,t)$表示连续的视频信号;$V(m\Delta_x,n\Delta_y,k\Delta_t)$表示离散的视频序列;$m,n,k$分别表示视频信号在水平方向、垂直方向及时间方向上的离散采样索引;$\Delta_x,\Delta_y,\Delta_t$分别表示空间水平采样间隔、空间垂直采样间隔及时间采样间隔.

1.2 数据融合与重构

本节主要介绍数据转换后的数据融合与重构过程,如图3所示.利用四维超混沌Chen系统[19],有效地融合异构数据.随后,所有数据通过数据抽象层,被构建为结构化的统一数据格式,进而为数据安全层中加密算法的设计奠定基础.

异构数据融合旨在将经过数据转换后的多类型数据按照一定规则组合为无序的数据序列.利用不同数据类型在数据规模和特性分布方面存在的显著差异,在初步确定基准数据源后,结合具有高复杂度、高敏感度及强抗攻击能力的四维超混沌Chen系统以及各类数据间的数量关系,对数据融合过程中的融合位置与融合数量进行动态调控.本文使用文献[19]中提出的改进的Chen混沌系统,其计算公式表示为

$$\left.\begin{aligned}\frac{\mathrm{d}x}{\mathrm{d}t}&=a(y-x),\\ \frac{\mathrm{d}y}{\mathrm{d}t}&=-dx-xz+cy-w,\\ \frac{\mathrm{d}z}{\mathrm{d}t}&=xy-bz,\\ \frac{\mathrm{d}w}{\mathrm{d}t}&=x+k.\end{aligned}\right\} \tag{5}$$

式中:a,b,c,d是混沌系统的控制参数,$a=36,b=3,c=28,d=16$;k是1个可调参数且$k\in[-0.5,0.5]$.

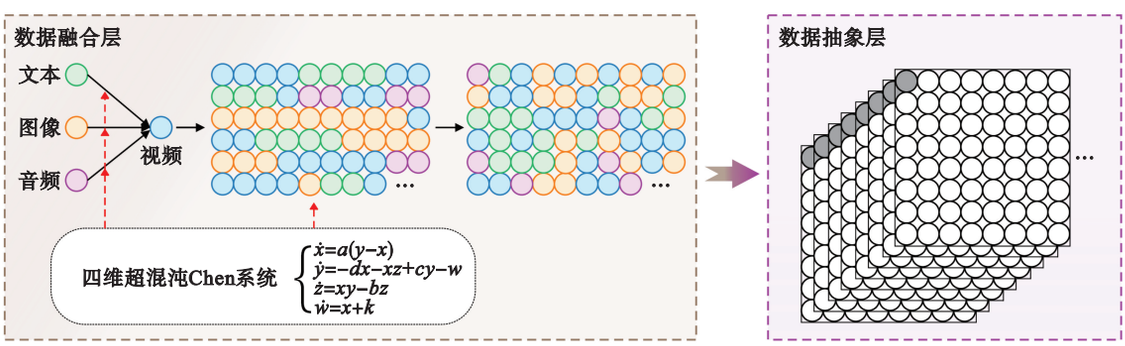


图3 数据的融合与重构示意图

Fig. 3 Schematic diagram of data fusion and reconstruction

以文本、图像、音频和视频4类数据作为输入源为例,首先分析4类数据的数据规模并选取数据量最大的类型作为融合的基准数据流(base stream, BS).随后,通过计算视频数据与文本、图像和音频数据之间的数量关系,确定文本、图像和音频数据在融合过程中的融合数量.为确定它们的融合位置,利用式(5)中生成的伪随机序列完成异构数据的动态融合操作,并按照既定比例将文本、图像和音频数据依次嵌入到视频流中.在此基础上,为了进一步降低明文数据之间的相关性,本文采用式(5)中生成的伪随机序列对明文数据进行置乱操作.通过该置乱过程,可以有效打乱明文数据的排列顺序,使融合后数据的统计特性呈均匀分布,从而显著提升抗统计攻击的能力.图3中的数据融合层给出了1个具体示例.该数据融合策略的提出,不仅打破了传统融合方案的有序性,而且保证了融合算法的可逆性.

融合后的数据输入到数据抽象层中,该层的核心逻辑是将不同类型数据统一为相同表现模式,实现数据的结构统一.首先,整体数据被分割为$\left\lceil\frac{l}{n\times n}\right\rceil$个等长序列,其中$l$表示融合后数据长度,$n=8$,如果最后一个等长序列中的元素个数$\alpha<n\times n$,为保证格式的统一化,在此序列末尾填充$n\times n-\alpha$个补充零值.然后,利用离散余弦变换(discrete cosine transform, DCT)将空域数据转换为频域数据,并进一步采用量化处理,从而有效降低数据冗余度.

1.3 密钥生成

由于分段线性混沌映射在概率分布密度、数值敏感度、实现复杂度等方面具有优良特性[18,20],本文首先利用分段线性混沌映射生成安全密钥为后续加密算法的设计提供基础支持.顾名思义,分段线性混沌映射的核心思想是将区间对称分割,通过点映射到区间,进而直观量化其动力学行为,数学形式表现为

$$x_{n+1}=F(x_n)=\begin{cases}\dfrac{x_n}{p}, & 0\leqslant x_n<p;\\ \dfrac{x_n-p}{0.5-p}, & p\leqslant x_n<0.5;\\ F(1-x_n), & 0.5\leqslant x_n<1.\end{cases}\tag{6}$$

式中：$F(\cdot)$为迭代映射函数；p为控制参数，当$p\in(0,0.5)$时，该混沌系统呈现混沌特性；当$n=0$时，x_0为初始值，取值范围在[0, 1]之间.

实验过程中，定义$p=0.319\,223\,802\,1$，$x_0=0.813\,512\,523\,8$，并对上述混沌映射算法迭代100 000次后，根据式(7)~(8)，分别生成2个密钥集k_{e1}，k_{e2}，用于加密低频系数和高频系数.

$$\bar{x}=\frac{1}{n}\sum_0^{n-1}x_n,\tag{7}$$

$$k_e=\begin{cases}0, & x_n\geqslant\bar{x},\\ 1, & x_n<\bar{x}.\end{cases}\tag{8}$$

式中：$\bar{x}$表示一组数的平均值；k_e表示生成密钥.

1.4　块级置乱方案

基于1.2节完成的数据融合与重构处理，为进一步降低重构后相邻序列之间的相关性，在数据抽象层处理结束后，对所有元素块进行连续双重置乱操作. 以m块为例，对块级置乱过程进行简单阐述，其流程如图4中块级置乱所示.

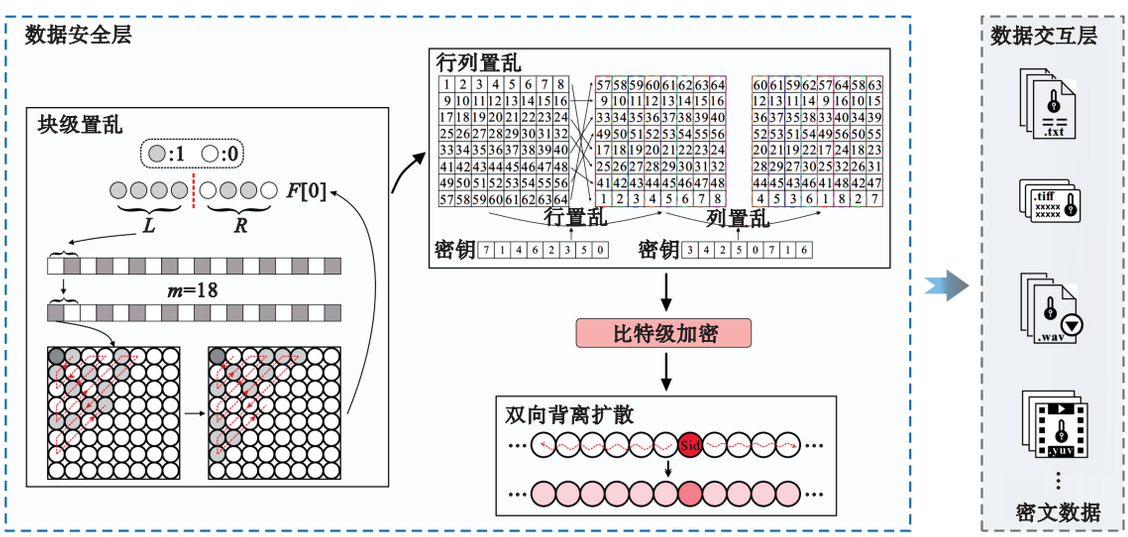


图4　安全算法设计与数据重构示意图

Fig. 4　Schematic diagram of secure algorithm design and data reconstruction

具体置乱算法如下：

步骤1　依次配对数据抽象层中生成的元素块，生成若干对，并定义初值$F[0]$作为反馈值，$F[0]\in[0,\ 1\,515]$.

步骤2　以2 b为单位分割$F[0]$，分割后的值分别定义为L和R，如果$L>7$，则当前对中的元素块进行1次交换操作；反之，则保持原始块状态不变.

步骤3　块交换完成后，针对性地处理块中存在的非零元素：

步骤3.1　提取块交换后第2个块中最后1个非零元素前的所有高频元素$A_1=\{p_1,p_2,p_3,\cdots,p_\tau\}$，其中，$p_\tau$表示当前块中最后1个非零元素，$0\leqslant\tau\leqslant62$. 计算该块中非零交流系数(AC)值个数$\gamma$并计算循环次数$S_L=L\%\gamma$，$0\leqslant\gamma\leqslant\tau$. 随后，循环左移$A_1$中的所有元素$S_L$次，得到$\widetilde{A_1}=\{p_{1+S_L},p_{2+S_L},\cdots,p_\tau,p_1,p_2,\cdots,p_{S_L}\}$. 最后拼接直流系数(DC)，$\widetilde{A_1}$和剩余的高频零元素、还原块形式定义为$C_1$.

步骤3.2　提取块交换后第2个块中第1个非零元素前的所有高频元素$A_2=\{p_1,p_2,p_3,\cdots,p_\tau\}$，其中，$p_\tau$表示当前块中最后1个非零元素，$0\leqslant\tau\leqslant62$. 计算该块中非零AC值个数$\gamma$并计算循环次数$S_R=(L+R)\%\gamma$，$0\leqslant\gamma\leqslant\tau$. 随后，循环左移$A_2$中的所有元素$S_R$次，得到$\widetilde{A_2}=\{p_{1+S_R},p_{2+S_R},\cdots,p_\tau,p_1,p_2,\cdots,p_{S_R}\}$. 最后拼接DC系数，$\widetilde{A_2}$和剩余高频零元素，还原块形式定义为$C_2$.

步骤4　更新反馈值$F[0]$，计算公式具体如下所示：

$$F[1]=(\mathrm{PS}(C_1,C_2))\ \mathrm{xor}\ F[0].$$

式中：PS(·)表示计算非零元素之和函数；xor表示异或操作.

步骤5　使用步骤4中更新的反馈值作为步骤1的输入，并循环步骤1至步骤4，直至所有对完成置乱操作.

步骤6 完成对间的块级置乱后,分别以行和列为单位进行基于密钥的块内行列置乱,进一步打破块间元素的相关性.置乱流程如图4中行列置乱所示.

1.5 比特级加密算法

大量实证研究表明,仅置乱的加密系统无法抵抗选择明文攻击[21-23].为了解决这一问题,在上述块级置乱后,采用比特级加密算法对m个8×8块中的低频系数进行加密.详细的加密算法如下:

步骤1 获取所有块中的低频系数,生成低频系数列表$L^{\mathrm{LF}}=\{l_i^{\mathrm{LF}}|i=0,1,\cdots,m-1\}$.

步骤2 将l_i^{LF}转化为8 b二进制表示,并以4 b为单位进行拆分,得到高位和低位.

步骤3 丢弃1.3节生成的k_{e1}前2 000个密钥以避免伪随机序列中的瞬态效应,随后,将剩余密钥逐位与高位元素进行异或操作.

步骤4 拼接步骤3中的计算结果和对应位置的低位元素,最后将拼接结果转化为十进制数,具体计算公式为

$$\widetilde{L^{\mathrm{LF}}}=\{\widetilde{l_i^{\mathrm{LF}}}|i=0,1,\cdots,m-1\}.$$

式中:$\widetilde{L^{\mathrm{LF}}}$表示加密后低频系数的集合;$\widetilde{l_i^{\mathrm{LF}}}$表示加密后的低频系数值.

1.6 双向背离扩散算法

对高频系数进行深入探究后,发现高频系数中存在大量零值系数,本文称之为"无意义系数".无意义系数占据了大量的存储空间,对其进行扩散操作无疑是增加了计算机的存储负担.因此,本文以非零高频系数为加密目标,设计了1种随机的双向背离扩散算法,用于进一步保护细节信息,如图4所示.该算法的核心思路是寻求一个扩散开端.利用1.5节中生成的密文低频系数计算加密非零高频系数的开始索引值Sid,具体步骤如下:

步骤1 计算低频系数均值$\overline{E^{\mathrm{LF}}}=\dfrac{1}{m}\sum_{i=0}^{m-1}\widetilde{l_i^{\mathrm{LF}}}$;

步骤2 获取差值最小值$\mathrm{MINLF}=\min(\widetilde{l_i^{\mathrm{LF}}}-\overline{E^{\mathrm{LF}}})$;

步骤3 寻找$\widetilde{L^{\mathrm{LF}}}$中最接近MINLF的索引值Sid.

通过上述步骤确定唯一Sid后,提取所有块中的非零高频系数并存放于列表$L^{\mathrm{HF}}=\{l_j^{\mathrm{HF}}|j=0,1,\cdots,\alpha-1\}$,其中$\alpha$表示非零高频系数总数.根据Sid将$L^{\mathrm{HF}}$中的$l_j^{\mathrm{HF}}$分为两部分$j=[0,\mathrm{Sid}]\cup(\mathrm{Sid},\alpha-1]$,最终采用式(9)生成密文非零高频系数,具体步骤如算法1所示.

$$\left.\begin{aligned}&\widetilde{l_j^{\mathrm{HF}}}=l_j^{\mathrm{HF}}\oplus\widetilde{k_{\mathrm{e2}}^{\beta}}, && j=\mathrm{Sid},\beta=0;\\&\widetilde{l_{j+1}^{\mathrm{HF}}}=\widetilde{l_{j+1}^{\mathrm{HF}}}\oplus\widetilde{l_j^{\mathrm{HF}}}\oplus\widetilde{k_{\mathrm{e2}}^{\beta+1}}, && j>\mathrm{Sid};\\&\widetilde{l_{j+1}^{\mathrm{HF}}}=\widetilde{l_{j+1}^{\mathrm{HF}}}\oplus\widetilde{l_j^{\mathrm{HF}}}\oplus\widehat{k_{\mathrm{e2}}^{\gamma+1}}, && j<\mathrm{Sid},\gamma=0.\end{aligned}\right\}\tag{9}$$

式中:$\widetilde{l_j^{\mathrm{HF}}}$表示加密后的非零高频系数;$\widetilde{k_{\mathrm{e2}}^{\beta}}$是$k_{\mathrm{e2}}$的变体,由$k_{\mathrm{e2}}$中每3个连续值组成的十进制值,表示右向扩散高频系数的密钥;$\widehat{k_{\mathrm{e2}}^{\gamma}}$同样是$k_{\mathrm{e2}}$的变体,由$k_{\mathrm{e2}}$中每2个连续值组成的十进制值,表示左向扩散高频系数的密钥.

算法1 双向背离扩散.

输入:$\widetilde{L^{\mathrm{LF}}}$,$k_{\mathrm{e2}}$,加密后的$n\times n$块.

输出:密文高频系数的Zigzag形式.

1.寻找起始索引Sid;

2.双向扩散非零高频系数,生成两部分密文集$\widetilde{LL^{\mathrm{HF}}}$,$\widetilde{RL^{\mathrm{HF}}}$;

3.组合$\widetilde{LL^{\mathrm{HF}}}$,$\widetilde{RL^{\mathrm{HF}}}$,最终生成密文非零高频系数集$\widetilde{L^{\mathrm{HF}}}=\widetilde{LL^{\mathrm{HF}}}+\widetilde{RL^{\mathrm{HF}}}$;

4.将$\widetilde{L^{\mathrm{HF}}}$还原到Zigzag后的形式.

2 性能分析

2.1 数据集与实验环境

本节主要以文本、图像、音频和视频作为测试对象,验证所提算法的有效性和合理性.测试数据的详细信息如图5和表1所示,图5a~5r依次对应表1(从上到下、从左到右)中的排列信息.文本采用英文、中文及混合文本进行测试,图像数据来源于常见的USC-SIPI数据集[24],音频数据下载于百度浏览器,视频数据由Xiph.Org基金会提供[25].其中,以.txt结尾的文本文件大小是经过UTF-8编码后的字节数,以.tiff结尾的图像文件分辨率均为256像素×256像素,大小则通过原始图像的长、宽和位深计算得出,以.wav结尾的音频数据大小是通过脉冲编码调制采样后得到的音频数据字节数,以.yuv结尾的视频数据,其大小即为该文件在计算机中实际占用的存储空间.所有实验运行于1台个人Windows计算机(Intel Core(TM) i7-9700 CPU,8 GB内存),编译环境为Pycharm 2021.

2.2 感知结果分析

有效的加密算法应用于原始数据后,应使原始内容在视觉或听觉感知上完全不可辨识.为了验证所提算法的有效性,本节分别以多输入源数

据（文本、图像、音频和视频）作为测试对象，进行加密实验，加密结果如图 6 所示．从图 6 中可以看出，加密后的混合文本（如图 6g 和 6k 所示）呈现出由数字、大小写字母以及基础数学符号组成的杂乱无序序列，原有语义结构被完全破坏，无法从中解析出任何信息，实现了文本内容的完全隐藏．密文图像（见图 6i）以及加密后视频第 1 帧（见图 6j）则呈现为类似噪声的均匀随机分布，原始图像中的视觉内容完全消失．将加密后的音频信号转化为可视化频率图后，可以观察到原始音频的频率特征在加密后完全消失，密文音频的频谱（见图 6h 和 6l）在一定频率范围内呈均匀分布，无法从中还原或推断出任何有效的原始音频信息．综上所述，所提的加密算法在混合文本、图像、音频和视频数据中均实现了明文内容的完全不可感知状态，验证了其在视觉和听觉层面具备良好的安全性能．



图 5　测试数据

Fig. 5　Test data

（a~c）—文本测试数据；（d~i）—图像测试数据；（j~l）—音频测试数据波形图；
（m~r）—foreman.yuv 视频测试数据图，依次为第 1 帧，第 10 帧，第 20 帧，第 30 帧，第 40 帧和第 50 帧．

表 1　测试数据详情

Table 1　Details of test data

名称	类型	大小/B	名称	类型	大小/B
英文文本	文本	838	4. 1. 08Jelly beans. tiff	图像	196 608
中文文本	文本	666	5. 1. 12Clock. tiff	图像	65 536
混合文本	文本	1 344	Bomb_plant_BL_A_1. wav	音频	113 488
4. 1. 01Female. tiff	图像	196 608	iPhone_message. wav	音频	50 000
256House. tiff	图像	196 608	QQ_Remind. wav	音频	28 336
4. 1. 03Female. tiff	图像	196 608	foreman. yuv	视频	108×10^5
Tree. tiff	图像	196 608			

2.3　效率分析

运行时间是评估加密算法可行性和实用性的关键指标之一．本节主要对所提加密算法的时间复杂度进行分析，并证明其在运行时间上的优势．本文提出的加密算法主要包括 4 个阶段：密钥生成、双重块级置乱、比特级低频系数加密和双向背离扩散，下面分别对每一阶段的时间复杂度展开分析．

在密钥生成阶段，本文使用分段线性混沌映射迭代 M 次后生成密钥，其时间复杂度为 $O(M)$，其中 M 表示迭代次数．在块级置乱过程中，所提算法设计了双重块级置乱方案．首先，以对的形式分别对块中的元素进行移动置乱，有选择地置乱块中相应元素，该过程中的时间复杂度为 $O\left(\frac{S}{64}\right)\approx O(S)$，其中，$S$ 表示数据的大小．其次，在上述基础上以行和列为单位进行块间置乱，此过程中的时间复杂度为 $O\left(\frac{S}{64}\right)\approx O(S)$．在比特级低频系数加密过程中，主要采用分割、异或、重组等手段完成，时间复杂度取决于低频系数的个数，计算为 $O\left(\frac{S}{64}\right)\approx O(S)$．在双向背离扩散阶段，本

加密方案主要加密所有非零高频系数,假设输入待加密数据中存在α个非零高频系数,该加密过程的时间复杂度为$O\left(\frac{S}{64}+\alpha\right)\approx O(S)$.

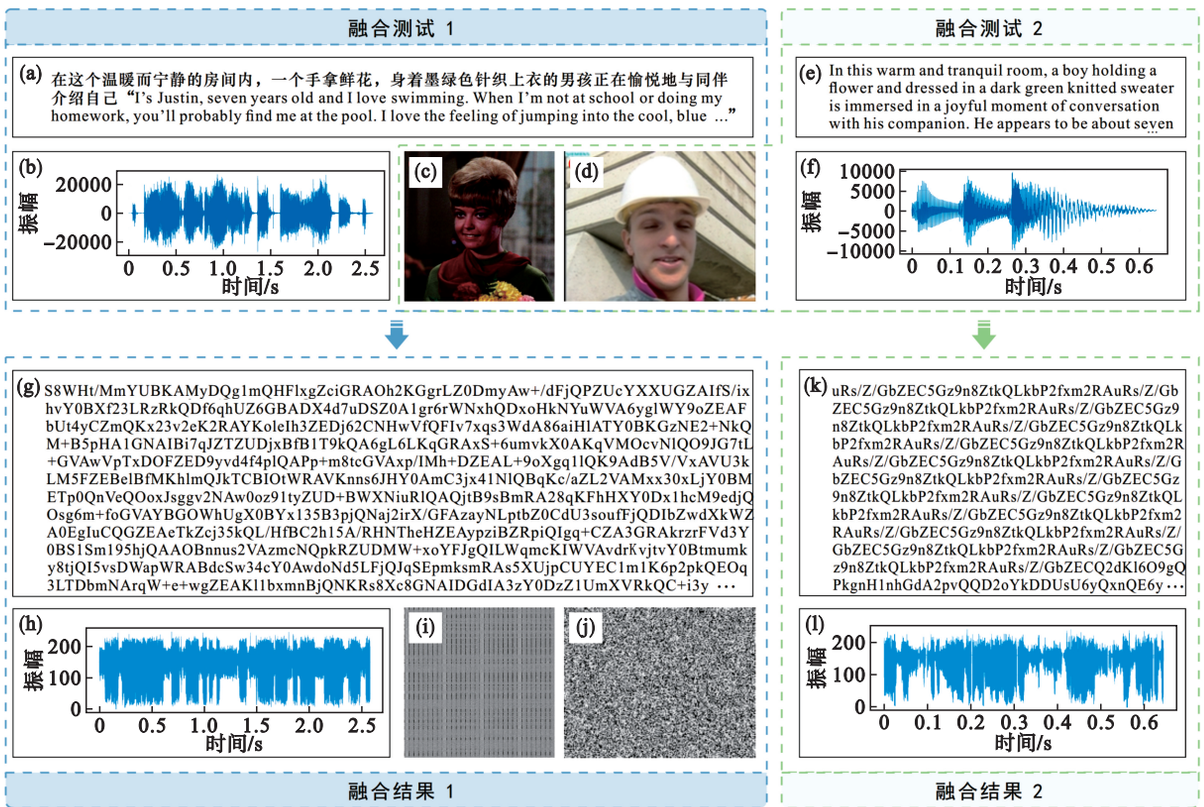


图6 明文与密文对比图

Fig. 6 Comparison diagram between plaintext and ciphertext

(a)—混合文本原始数据;(b)—Bomb_plant_BL_A_1.wav采样图;(c)—4.1.01Female.tiff;(d)—foreman.yuv(第1帧);(e)—英文文本原始数据;(f)—QQ_Remind.wav采样图;(g)—(a~d)混合加密后提取的文本密文结果;(h)—(a~d)混合加密后提取的音频密文结果;(i)—(a~d)混合加密后提取的图像密文结果;(j)—(a~d)混合加密后提取的视频第1帧密文结果;(k)—(c~f)混合加密后提取的文本密文结果;(l)—(c~f)混合加密后提取的音频密文结果.

综上所述,本加密方法的整体时间复杂度为$O(M)+O(S)+O(S)+O(S)+O(S)=O(M+S)$,主要取决于输入待加密数据的大小以及生成密钥的循环次数(M),当M远远小于待加密数据的大小时,本加密方法的时间复杂度可简化为$O(S)$,对资源有限的软硬件设备较友好.

2.4 直方图分析

直方图反映数值在一定区间内的分布规律,通过分析密文直方图的分布情况,可以直观地量化加密算法对原始数据的改变程度.当直方图呈均匀分布时,攻击者无法通过其数据分布推断原始像素的分布状态;反之,攻击者可以通过直方图中数据的峰值推断原始数据的分布规律,进而攻破加密算法,直接获取原始数据,造成重要数据泄露.图7展示了4类数据的明文与对应的密文分布直方图,其中,使用字节直方图表示文本与音频的数据分布,使用像素直方图表示图像的数据分布.从图7i中可以看出,密文图像的直方图分布呈均匀分布特征,灰度值出现的频率趋于一致且没有较为明显的峰值和低谷,原始图像的统计规律完全被打破.文本数据的密文直方图7g和7k虽然没有均匀分布于整个横坐标轴上,但在局部区域内呈现集中均匀状态,其分布模式与明文直方图完全不同,无法通过密文直方图定位原始文本的位置及结构特征.图7b和7f表示原始音频的分布形态,其值呈规律状态分布于0~255区间内,这主要是由于音频的采样存在一定的规律性和重复性,为攻击者提供了潜在的突破点.加密后音频的直方图分布(见图7h和7l)则呈现出完全不同于原始数据的分布形态,成功隐藏了原始音频的统计特征.

2.5 相关性分析

相关性一般用于测量相邻元素之间的近似程度,图像中的相关性称为像素相关性.对于1张

色彩丰富且画质细腻的图像而言，其相邻像素表现极为密切甚至相似，量化后的结果接近1，详细计算公式见文献[26]. 通常情况下，随机选取明文和密文中相同数量的像素，计算其在水平、垂直和对角方位的相关性，其值若无限接近0，则表明提出的加密算法较好地消除了像素间的强相关性. 实验过程中，文本和音频数据的相邻相关性采用文献[7]中的计算方法，分别对任意元素 V_n 及其前后元素进行测试，实验结果如表2所示. 其中，密文文本的元素相关性存在于区间[0.010, 0.014]，密文图像和密文视频的第1帧像素相关性系数分别为0.027和−0.018左右，而密文音频的元素相关性的均值约为−0.4. 综上所述，4类数据的混合相关性均值为−0.127 6. 4类差异化数据经过提出的加密算法处理后，呈现出较弱的内容相关性，表明该加密算法具有较高的安全性.

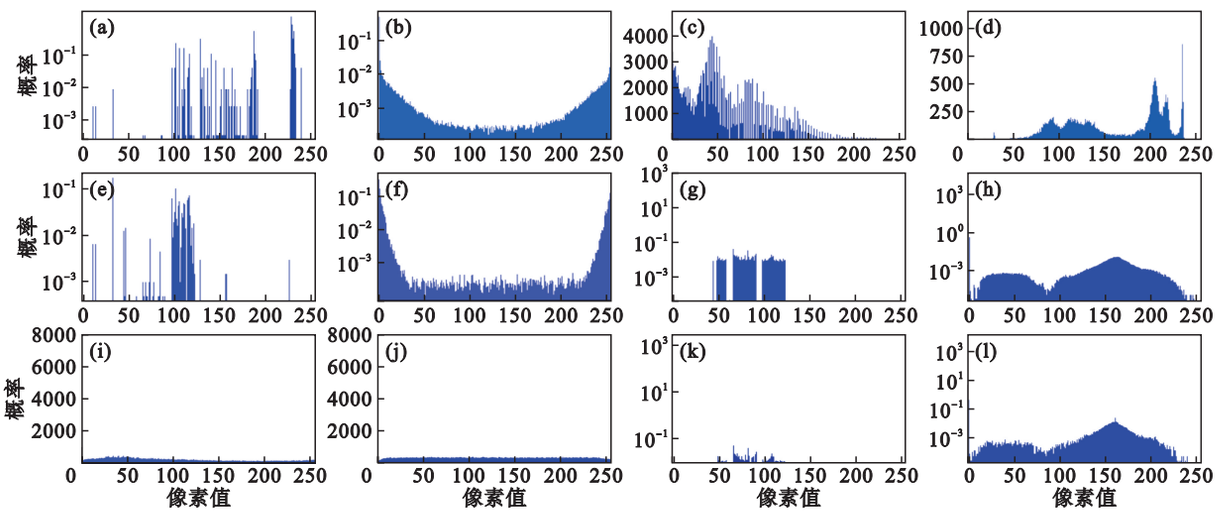


图7　明文与密文直方图比较

Fig. 7　Histogram comparison between plaintext and ciphertext

(a)—混合文本明文直方图；(b)—Bomb_plant_BL_A_1.wav明文直方图；(c)—4.1.01Female.tiff明文直方图；(d)—foreman.yuv原始视频第1帧；(e)—英文文本明文直方图；(f)—QQ_Remind.wav明文直方图；(g)—(a~d)混合密文文本直方图；(h)—(a~d)混合密文音频直方图；(i)—(a~d)混合密文图像直方图；(j)—(a~d)混合密文视频第1帧直方图；(k)—(c~f)混合密文文本直方图；(l)—(c~f)混合密文音频直方图.

表2　多源异构数据的相关性系数分析

Table 2　Analysis of correlation coefficients of multi-source heterogeneous data

名称	明文相关性系数		混合密文相关性系数	
	V_n, V_{n-1}	V_n, V_{n+1}	V_n, V_{n-1}	V_n, V_{n+1}
混合文本	0. 868 9	0. 867 8	0. 014 4	0. 014 5
Bomb_plant_BL_A_1. wav	0. 882 7	0. 882 7	−0. 407 0	−0. 407 0
4. 1. 01Female. tiff	0. 964 0		0. 027 7	
foreman. yuv(第1帧)	0. 959 0		−0. 018 3	
英文文本	−0. 110 7	−0. 112 2	0. 010 3	0. 010 3
QQ_Remind. wav	0. 978 5	0. 978 5	−0. 393 0	−0. 393 0

注：对于文本和音频数据，其相关性通过计算任意元素 V_n 与其相邻元素 V_{n-1} 和 V_{n+1} 之间的相关性系数获得；图像和视频数据，则随机选取3 000对相邻像素值进行相关性测量.

2.6　信息熵分析

信息熵是一种用于评估数据复杂度的通用测量指标[27-28]. 使用UTF-8编码的文本、音频、图像和视频的信息熵取值范围通常在0~8之间，其值越接近8时，表明该组数据中信息量越大，相关性越弱. 反之，数据信息越平整且相关性越强. 一般地，研究者期望密文数据的信息熵无限接近8，这表明算法具有较好的信息扰动能力，信息熵计算方法如式(10)所示. 表3展示了部分测试数据的明文信息熵和密文信息熵，可以得到密文信息熵均值为7.484 07. 测试结果表明，使用提出的加密算法对4类数据进行加密后，原始数据的统计

特征被有效隐藏,表明加密算法具有较强的抗统计分析能力.

$$H=-\sum_{i=0}^{255}p(x_i)\mathrm{lb}(p(x_i)). \tag{10}$$

式中:x_i表示元素值;$p(x_i)$表示x_i出现的概率;lb(·)表示以2为底的计算函数.

表3 多源异构数据的信息熵

Table 3 Information entropy of multi-source heterogeneous data b

名称	明文信息熵	混合密文信息熵
混合文本	5.986 2	7.353 0
Bomb_plant_BL_A_1.wav	3.166 2	7.382 5
4.1.01Female.tiff	7.056 5	7.531 2
foreman.yuv(第1帧)	7.146 1	7.965 0
英文文本	4.267 0	7.323 9
QQ_Remind.wav	3.083 2	7.348 8

2.7 差分攻击分析

差分攻击是通过分析微小差异进而攻破加密算法的一种手段.本节以密钥和明文作为测试内容,以NPCR(number of pixels change rate)和UACI(unified average changing intensity)作为检验指标(具体计算方式见式(11)~(12)[29-30]),验证所提算法对差分攻击的抵抗能力.首先,分别使用不同密钥(原始密钥和仅改变1 b的密钥)加密相同的目标载体,NPCR和UACI测试结果如表4中前两行所示,NPCR和UACI均值分别为98.73%和32.98%,二者都接近既定最优值(99.60%和33.46%),表明所提算法具有一定的密钥敏感性.其次,使用相同密钥分别加密不同明文数据(明文数据和仅改变1 b的近似数据),若生成2个完全不同的密文列表,则表明所提算法具有一定抵抗明文攻击的能力.量化结果如表4中后两行所示,从中可以看出密文数据的NPCR和UACI均值(99.01%和32.92%)在最优理论值上下浮动,表明加密算法具有一定的抗明文攻击能力.

$$\mathrm{UACI}=\frac{1}{n}\left[\sum_j\frac{\left|C_1(j)-C_2(j)\right|}{255}\right]\times 100\%, \tag{11}$$

$$\mathrm{NPCR}=\frac{\sum_j E(j)}{n}\times 100\%. \tag{12}$$

式中:$E(j)=\begin{cases}1, C_1(j)\neq C_2(j)\\ 0, C_1(j)=C_2(j)\end{cases}$;$C_1(j)$和$C_2(j)$表示不同文件中相同位置的元素值;$n$表示元素值的总个数.

表4 密钥敏感性和明文敏感性分析

Table 4 Analysis of key sensitivity and plaintext sensitivity %

测试内容	指标	混合文本	Bomb_plant_BL_A_1.wav	4.1.01Female.tiff	英文文本	QQ_Remind.wav
密钥敏感性	NPCR	99.531 2	97.312 1	99.105 4	99.536 1	98.207 0
	UACI	33.152 2	32.280 5	33.228 1	33.210 3	33.050 0
明文敏感性	NPCR	99.051 1	98.831 0	99.100 6	99.183 4	98.893 3
	UACI	33.411 8	32.081 4	33.281 0	32.915 8	32.957 1

3 结 语

本文设计了1个面向多源异构数据的轻量级安全加密框架.针对多源异构数据的特征,通过数据融合层和数据抽象层将文本、图像、音频、视频等数据进行融合,然后构建1个通用结构体.抽象出的数据经过数据安全层,融合混沌加密算法,以保障明文数据在物联网中的安全传输.在安全层中,多源数据首先以块为单位进行双重块级置乱来破坏数据的原始位置;此外,通过比特级加密算法以及双向背离扩散等操作,彻底将置乱后的数据转化成"伪数据",以应对非法用户的未授权访问与数据重建.实验结果表明,所提算法对不同类型数据源均表现出良好的安全性.由于该算法利用轻量级混沌映射生成伪随机密钥,大大降低了数据操作中的时间消耗,较好地满足了用户对实时性的需求,可以部署和应用于任意计算机.然而,当采样数据为波动较小的音频时,不可避免地面临数据融合有限、采样值变化范围有限等问题,这将是未来着重考虑和攻克的问题之一.

参考文献:

[1] 余辉, 梁镇涛, 鄢宇晨.多来源多模态数据融合与集成研究进展[J].情报理论与实践, 2020, 43(11): 169-178.
(Yu Hui, Liang Zhen-tao, Yan Yu-chen. Review on multi-source and multi-modal data fusion and integration [J]. *Information Studies* (*Theory & Application*), 2020, 43(11): 169-178.)

[2] Zheng Y. Methodologies for cross-domain data fusion: an overview[J]. *IEEE Transactions on Big Data*, 2015, 1(1): 16-34.

[3] Bleiholder J，Naumann F. Data fusion[J]. *ACM Computing Surveys*，2009，41(1)：1-41.

[4] 李仁正，高冠东，宋胜尊，等. 基于改进的FGM-CM-BERT模型多模态情感分析方法[J]. 河北大学学报(自然科学版)，2025，45(2)：192-203.
(Li Ren-zheng，Gao Guan-dong，Song Sheng-zun，et al. Multimodal sentiment analysis method based on improved FGM-CM-BERT model [J]. *Journal of Hebei University (Natural Science Edition)*，2025，45(2)：192-203.)

[5] Wan Z S，Du Y H，Ibrahim M，et al. Thinking and moving：an efficient computing approach for integrated task and motion planning in cooperative embodied AI systems (invited paper) [C]//2024 ACM/IEEE International Conference on Computer Aided Design (ICCAD). Newark，2025：1-7.

[6] Huang Y Y，Hao Y H，Yu B，et al. Dadu-corki：algorithm-architecture co-design for embodied AI-powered robotic manipulation [C]//Proceedings of the 52nd Annual International Symposium on Computer Architecture. Tokyo，2025：327-343.

[7] 周双，尹彦力，王诗雨，等. *n*维离散超混沌系统及其在音频加密中的应用[J]. 物理学报，2024，73(21)：35-44.
(Zhou Shuang，Yin Yan-li，Wang Shi-yu，et al. An *n*-dimensional discrete hyperchaotic system and its application in audio encryption [J]. *Acta Physica Sinica*，2024，73(21)：35-44.)

[8] 杨晓晖，贾凯. 基于区块链的医疗数据可信共享方案[J]. 河北大学学报(自然科学版)，2024，44(3)：322-328.
(Yang Xiao-hui，Jia Kai. A blockchain-based trusted data sharing scheme for electronic medical records[J]. *Journal of Hebei University (Natural Science Edition)*，2024，44(3)：322-328.)

[9] Matthews R. On the derivation of a "chaotic" encryption algorithm[J]. *Cryptologia*，1989，13(1)：29-42.

[10] Fridrich J. Image encryption based on chaotic maps [C]// 1997 IEEE International Conference on Systems，Man，and Cybernetics，Computational Cybernetics and Simulation. Orlando，1997：1105-1110.

[11] Tang Z，Yin Z X，Yang J，et al. Information encryption scheme based on chaotic map and hybridization chain reaction[J]. *Journal of Physics：Conference Series*，2021，2026(1)：012013.

[12] Zhu D，Tong X J，Wang Z，et al. A novel lightweight block encryption algorithm based on combined chaotic system[J]. *Journal of Information Security and Applications*，2022，69：103289.

[13] Wu X J，Kan H B，Kurths J. A new color image encryption scheme based on DNA sequences and multiple improved 1D chaotic maps[J]. *Applied Soft Computing*，2015，37：24-39.

[14] Yu J W，Xie W，Zhong Z Y，et al. Image encryption algorithm based on hyperchaotic system and a new DNA sequence operation[J]. *Chaos*，*Solitons & Fractals*，2022，162：112456.

[15] Signing F V R，Fonzin F T，Kountchou M，et al. Chaotic jerk system with hump structure for text and image encryption using DNA coding [J]. *Circuits*，*Systems*，*and Signal Processing*，2021，40(9)：4370-4406.

[16] 魏雅娟，范九伦，任方. 基于混沌和小波变换的音频加密算法[J]. 计算机科学，2017，44(12)：94-99.
(Wei Ya-juan，Fan Jiu-lun，Ren Fang. Audio encryption algorithm based on chaos and wavelet transform [J]. *Computer Science*，2017，44(12)：94-99.)

[17] Zhao R Y，Zhang Y S，Ji J H，et al. AES-AUDIO：an encryption scheme for audio supporting differentiated decryption [J]. *IEEE Transactions on Multimedia*，2025，27：2268-2280.

[18] Li S J，Chen G R，Mou X Q. On the dynamical degradation of digital piecewise linear chaotic maps [J]. *International Journal of Bifurcation and Chaos*，2005，15(10)：3119-3151.

[19] Gao T G，Gu Q L，Chen Z Q. Analysis of the hyper-chaos generated from Chen's system [J]. *Chaos*，*Solitons & Fractals*，2009，39(4)：1849-1855.

[20] Tian J F，Lu Y，Zuo X Y，et al. A novel image encryption algorithm using PWLCM map-based CML chaotic system and dynamic DNA encryption [J]. *Multimedia Tools and Applications*，2021，80(21)：32841-32861.

[21] Li S J，Li C Q，Chen G R，et al. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks [J]. *Signal Processing：Image Communication*，2008，23(3)：212-223.

[22] Jolfaei A，Wu X W，Muthukkumarasamy V. On the security of permutation-only image encryption schemes [J]. *IEEE Transactions on Information Forensics and Security*，2016，11(2)：235-246.

[23] Li C Q，Lo K T. Optimal quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks[J]. *Signal Processing*，2011，91(4)：949-954.

[24] Weber A G. The USC-SIPI image database version 5 [EB/OL]. (1997-01-01) [2026-01-18]. https://www.researchgate. net/publication/242578505_Usc-sipi_image_database_version_5.

[25] Montgomery C. Xiph. org test media [EB/OL]. [2026-03-08]. https://media.xiph.org/.

[26] Xing M，Yu H，Zhang W，et al. Parallelizable chaotic encryption for remote sensing imagery [J]. *International Journal of Bifurcation and Chaos*，2024，34(16)：2450207.

[27] Chen Z，Chen Z，Long B F，et al. A cross-channel color image encryption scheme based on a novel 4D hyperchaotic system and 3-layer Peano curve [J]. *Expert Systems with Applications*，2026，309：131145.

[28] Liu X B，Yang J. Joint JPEG compression and encryption with DC groups' random cross-permutation and ZRVs' inter-block permutation [J]. *IEEE Transactions on Multimedia*，2026，28：373-387.

[29] Tang M，Guo D，Lin Y Y. A novel multi-color image compression encryption algorithm based on the reconstruction coefficient matrix and DNA point mutation operation[J]. *Expert Systems with Applications*，2025，270：126620.

[30] Wang Q，Yang Y L，Zhang X Q. Real-time medical image encryption algorithm based on punch scrambling and fast Hachimoji DNA coding [J]. *Expert Systems with Applications*，2026，309：131207.