n 维离散超混沌系统及其在音频加密中的应用*

周双[1)†] 尹彦力[1)] 王诗雨[1)] 张盈谦[2)3)]

1) (重庆师范大学数学科学学院, 重庆 401331)

2) (厦门大学嘉庚学院, 漳州 363105)

3) (厦门大学马来西亚分校, 雪邦 43900, 马来西亚)

(2024 年 7 月 24 日收到; 2024 年 8 月 26 日收到修改稿)

与现有其他混沌系统不同, 本文探索了一种具有简单结构的 n 维离散超混沌系统. 首先, 利用正弦函数和幂函数以及简单运算构建 n 维离散超混沌系统; 然后, 理论分析该系统可以设置正的 Lyapunov 指数; 接下来, 以六维混沌系统为例, 对其进行了相图、分岔图、Lyapunov 指数、复杂性等动力学特征分析; 最后, 将新的混沌系统结合前后项异或运算和真随机数构建一次一密音频加密新方法. 通过实验仿真, 所提出的算法与现有音频加密算法进行比较, 该算法具有更高安全性, 能够抵御各种常见攻击.

关键词: 离散超混沌系统, Lyapunov 指数, 音频加密, K-means 算法

PACS: 05.45.Pq, 05.45.Vx **DOI:** 10.7498/aps.73.20241028

CSTR: 32037.14.aps.73.20241028

1 引 言

在 21 世纪的信息时代, 以网络和移动设备为代表的信息技术和产品越来越普及. 信息已成为世界和个人的重要资源, 信息安全也越来越成为人们关注的焦点. 目前, 经过时间和实践的检验, 已经存在大量成熟的加密算法, 如数据加密标准、高级加密标准等. 这些算法经过层层分析和测试, 有的通过严格的混淆和扩散操作以及足够的密钥长度来保证安全性, 有的则通过复杂的数论构造或计算数学难题来实现安全加密. 然而, 它们大多是以加密文本信息为出发点来设计和实现的, 因此在处理数据量关联度高的多媒体信息时, 加密效率和加密性能之间的矛盾就变得尤为突出.

在多媒体信息中, 音频文件的数据量通常大于图像或文本, 且相邻音频数据之间具有强相关性和高冗余度的特点, 但一些传统加密方法并非针对数字音频的特点而设计, 因此不适合专门对音频数据进行加密. 近年来, 越来越多的研究人员致力于音频加密技术的研究[1,2]. 例如, Yu 等[3] 提出了一种新的分数阶混沌系统, 并将其应用在双通道音频加密, 取得了较好的效果. Wu 等[4,5] 提出了一种基于 2 维混沌的音频单通道和双通道加密算法, 并使用相关数据集进行了评估, 表明其能够显著降低音频信息的时间相关性. Rahul 等[6] 利用生物特征图像和 SHA-256 哈希算法提出了一种基于混沌的音频加密算法. Demirtaş[7] 提出了一种基于混沌 Chebyshev 映射的无损安全音频加密方法. Liu[8] 提出了一种使用具有自适应参数扰动的 3D混沌系统的分块快速音频块加密方法. Cao 和 Liu[9] 提出了一种基于整数域 2D 无简并超混沌系统的一次一密的双通道音频加密方法. 然而大多数方法将构造的混沌系统作为伪随机序列发生器, 把产生的混沌序列与需要加密的音频信息 (明文) 进行简单的整体异或加密, 这样产生的密文安全性仅依赖混沌序列

* 重庆市自然科学基金 (批准号: CSTB2023NSCQ-MSX0401) 资助的课题.

† 通信作者. E-mail: zhoushuang@cqnu.edu.cn

的性能, 若某一部分被攻击者成功破解, 就会面临整体被破解的风险. 尽管密文的时域频域图在某些情况下与明文相比存在显著差异, 但由于加密是整体进行的, 播放密文音频时, 仍然能够辨识出其中的规律或捕捉到音频所携带的关键信息, 因此无法有效地保护明文信息的安全. 因此, 如何设计出一个高安全性的音频加密方法仍是目前研究的一个重点.

混沌系统具有伪随机性、对初始条件敏感的依赖性、遍历性等特点, 使其在很多领域得到应用, 并吸引了许多研究者对其进行研究[10–14]. 在保密通信中, 混沌系统也能作为一种有效的伪随机信号产生源, 在加密中起到重要作用. 因此, 构造性能好的新型离散超混沌系统是有意义的. 现有的一些经典的低维离散混沌系统, 如 Logistic 映射和 Tent 映射, 虽然简单, 但这些映射容易退化, 不再适合于现阶段的信息安全. 因此, 为了使离散混沌系统适用于密码学, 一些研究人员通过各种方法构造了抗退化能力的离散超混沌系统, 但是随着维数的增加, 设计难度也相应增加. 目前, 已经有了一些研究成果. 例如, Hua 等[15] 通过分析高维离散混沌映射的参数矩阵与其 Lyapunov 指数之间的关系构建了 n 维多项式函数的超混沌系统 (nD-PCS). Huang 等[16] 提出了基于忆阻器的抗退化 n 维离散超混沌系统. Fan 与 Ding[17] 通过 SVD 分解和模运算构造 n 维离散非退化超混沌映射. Zhao 与 Liu[18] 通过高斯消元法和模运算构造 n 维离散超混沌系统 (nD-NDHCM). Zhang 等[19] 提出了基于格什戈林圆盘定理的 n 维超混沌系统 (nD-HCM). Ding 等[20] 提出了可控 Lyapunov 指数范围的 n 维超混沌系统. 在前人研究的基础上, 为了优化系统结构, 减少函数项数和运算, 本文设计了一种新型 n 维离散超混沌系统, 与现有系统相比, 具有简单的结构、较高的复杂性和高效的运行效率. 最后, 将此混沌系统应用在音频加密中, 提出了一种结合前后项异或扩散和真随机数的音频加密算法, 并与现有加密算法进行对比, 来验证其有效性和较高的安全性.

2 预备知识

2.1 Lyapunov 指数

Lyapunov 指数表征相空间内系统相邻轨迹的平均发散程度, 是用来判断非线性系统状态的一种有效方法. 对于 n 维的混沌系统:

$$F(x)=\begin{cases} x_{n+1}^{(1)}=F_1\left(x_n^{(1)},\cdots,x_n^{(N)}\right), \\ x_{n+1}^{(2)}=F_2\left(x_n^{(1)},\cdots,x_n^{(N)}\right), \\ \vdots \\ x_{n+1}^{(N)}=F_N\left(x_n^{(1)},\cdots,x_n^{(N)}\right). \end{cases} \tag{1}$$

我们通过以下公式计算得到系统的 Lyapunov 指数:

$$\mathrm{LE}_j=\lim_{t\to\infty}\frac{1}{t}\ln|\lambda_j|,\quad j=1,2,\cdots,N, \tag{2}$$

其中 $\lambda_1,\lambda_2,\cdots,\lambda_N$ 是矩阵 $\boldsymbol{J}=\boldsymbol{J}(x_1)\boldsymbol{J}(x_2)\cdots\boldsymbol{J}(x_t)$ 的特征值, $\boldsymbol{J}(x_n)$ 是 $F(x)$ 的雅可比矩阵. 当非线性有界的系统具有正的 Lyapunov 指数时, 该系统处于混沌状态. 当有界的非线性系统具有两个或两个以上的正 Lyapunov 指数时, 该系统是超混沌的, 而且它会有更复杂的动力学行为和抗退化的能力.

2.2 K-means 算法

K-means 算法是由 MacQueen[21] 提出, 它是一种迭代性聚类算法, 对一个 n 维向量的数据点集 D 进行聚类:

$$D=\{x_i|i=1,2,\cdots,N\}, \tag{3}$$

其中 x_i 表示第 i 个数据点, 最终将集合 D 划分成 k 个类簇. 我们通常用欧式距离来衡量紧密度, 用误差平方和作为度量聚类质量的目标函数, 通过最小化目标函数, 将数据点按照距离聚类中心远近分成 k 个簇.

2.3 加密算法安全性分析方法

本部分介绍了本文运用的几种安全性分析方法, 包括差分攻击、相关系数、信息熵、鲁棒性和选择明文攻击.

1) 相关性分析

原始音频的相邻像素值之间具有很强的相关性, 而加密后的相邻像素值的相关性应尽可能小以抵御统计攻击. 为此, 我们使用相关系数指标来进行衡量, 它的计算公式为 $r(p,q)=\dfrac{\mathrm{cov}(p,q)}{\sigma(p)\sigma(q)}$, 其中 q 为 p 的相邻元素.

2) 信息熵分析

信息熵来衡量信息的混乱程度, 一个好的加密

算法, 密文的信息熵越大, 表示信息越混乱, 那么信息泄漏的可能性就越小. 它的公式计算如下所示:

$$H(s)=\sum_{i=0}^{2^L}P(s_i)\log_2\frac{1}{P(s_i)}, \tag{4}$$

其中 $P(s_i)$ 表示 s_i 发生的概率.

3) 鲁棒性分析

在信息传播过程中, 密文信息有可能部分丢失或者被噪声污染, 这就要求设计的加密算法能够在密文发生缺失或者污染时, 还能够解密出明文关键信息, 因此需要对算法进行鲁棒性分析.

4) 选择明文攻击分析

目前, 常见的四种攻击方式是已知密文攻击、已知明文攻击、选择明文攻击和选择密文攻击. 其中最具破坏性的是选择明文攻击. 如果一种加密算法能抵御指定明文攻击, 就能抵御四种常见攻击[4]. 假设 A_1 和 A_2 是原始音频信息, C_1 和 C_2 是加密后的音频信息. 当 $\lfloor A_1(i,j)\rfloor\oplus\lfloor A_2(i,j)\rfloor\neq\lfloor C_1(i,j)\rfloor\oplus\lfloor C_2(i,j)\rfloor$, 这表明加密算法可以抵御选择明文攻击[4].

3 n 维离散超混沌系统

3.1 超混沌系统构建

为了克服现有离散超混沌的一些缺点, 提出一种具有全局有界的 nD $(n\geqslant 3)$ 离散超混沌映射模型. 由于正弦函数可以产生全局有界限的复杂轨迹, 在此基础上, 该模型通过正弦运算可以构建超混沌系统. 此外, 鉴于许多研究学者在一些混沌系统使用了幂指数取得了很好的成果[15,18,19]. 同时使系统适用在保密通信领域, 又具有更多的密钥参数, 因此, 设置了幂指数参数 c_{ij}. 其定义为

$$F(x(i)):\begin{cases}x_1(i+1)=\sin(ra_{11}x_1(i)^{c_{11}}+a_{12}x_2(i)^{c_{12}}+b_1),\\ x_2(i+1)=\sin(ra_{22}x_2(i)^{c_{22}}+a_{23}x_3(i)^{c_{23}}+b_2),\\ \quad\vdots\\ x_{n-1}(i+1)=\sin(ra_{(n-1)(n-1)}x_{n-1}(i)^{c_{(n-1)(n-1)}}+b_{n-1}),\\ x_n(i+1)=\sin(a_{n2}x_2(i)^{c_{n2}}+\cdots+ra_{nn}x_n(i)^{c_{nn}}+b_n),\end{cases} \tag{5}$$

其中 $x_1,x_2,\cdots,x_n\in[-1,1]$, $c_{ij}\in Z^+$, $i,j\in N$, $a_{ij},r\in R-\{0\}$, $b_i\in R$.

下面通过调整设置参数可以推导出构建的混沌系统可以拥有 n 个正的 Lyapunov 指数.

$$\boldsymbol{J}(x(i))=\begin{pmatrix}ra_{11}c_{11}f_1 & a_{12}c_{12}f_1 & \cdots & 0\\ 0 & ra_{22}c_{22}f_2 & \cdots & 0\\ \vdots & \vdots & \ddots & 0\\ 0 & ra_{n2}c_{n2}f_n & \cdots & ra_{nn}c_{nn}f_n\end{pmatrix}, \tag{6}$$

其中 $f_i\,(i=1,2,\cdots,n)$ 表示 $F(x)$ 的每行外层函数的导数. 接下来, 计算 $\boldsymbol{J}(x(i))$ 的特征根:

$$|\lambda\boldsymbol{E}_{n\times n}-\boldsymbol{J}(x(i))|=(\lambda-ra_{11}c_{11}f_1)(\lambda-ra_{22}c_{22}f_2)\cdots(\lambda-ra_{nn}c_{nn}f_n)=0,$$

其中主对角线元素 $ra_{kk}c_{kk}f_k$ 决定 $\boldsymbol{J}(x(i))$ 的第 k 个特征值为 $\lambda_k^{x(i)}$, 因此, (6) 式的第 k 个 Lyapunov 指数可计算为

$$\mathrm{LE}_k=\lim_{t\to\infty}\frac{1}{t}\sum_{i=0}^{t-1}\ln\left|\lambda_k^{x(i)}\right|=\lim_{t\to\infty}\frac{1}{t}\sum_{i=0}^{t-1}\ln|ra_{kk}c_{kk}f_k|. \tag{7}$$

由于有计算机的有限位数和数据长度的限制, 通过设置 $|ra_{kk}c_{kk}f_k|>1$ 就能使得所有 Lyapunov 指数大于 0. 因此, 在计算机精度允许的范围内, 通过设置系统参数, 可以得到相应的 n 个正 Lyapunov 指数.

接下来, 我们比较不同方法的时间复杂度, 如表 1 所列. 可以推断出, 与现有方法对比, 新混沌系统的构建所需项数最少, 不涉及矩阵乘法, 具有较高的执行效率.

3.2 动力学特征分析

为了证明构建的混沌系统的有效性, 构造了由上述系统生成的 6D 混沌映射并分析了它们的动态行为, 其系统动力学表达式为

$$F(x(i)):\begin{cases} x_1(i+1)=\sin(r137x_1(i)+44x_2(i)^4), \\ x_2(i+1)=\sin(r157x_2(i)+94x_3(i)^4), \\ x_3(i+1)=\sin(r136x_3(i)+67x_4(i)^4), \\ x_4(i+1)=\sin(r129x_4(i)+98x_5(i)^4), \\ x_5(i+1)=\sin(r36x_5(i)), \\ x_6(i+1)=\sin(59x_2(i)+144x_3(i)^2 \\ \qquad +86x_4(i)^3+105x_5(i)^4 \\ \qquad +r59x_6(i)). \end{cases} \tag{8}$$

随机给参数 r 一个值, (8) 式混沌系统的状态点在三维相空间中的分布如图 1 所示, 由此可以推断其动态演化产生的状态点充满整个空间, 说明它具有较好的遍历性.

从图 1 看出迭代的序列分布在整个参数区间, 此时处于混沌状态.从 图 2 分岔图可以看出构建的映射没有出现分岔现象, 而是充满整个平面, 说明该系统具有连续混沌特性的参数空间.

1) Lyapunov 指数

在实验中, 通过设置合适的参数, Lyapunov 指数就不会为负. 如图 3 所示, 随着 r 的变化, 可以使系统有 6 个正 Lyapunov 指数.

2) 初值敏感性

我们对构建的六维混沌系统的初始值 x_1, x_2, x_3, x_4, x_5, x_6 做一个微小的扰动, 从图 4 可以看到, 如果初始值受到轻微扰动, 就会产生完全不同轨迹的混沌序列, 这说明该系统对初始值非常敏感.

表 1 不同方法的时间复杂度对比

Table 1. Comparison of time complexity of different methods.

离散混沌系统	元素加法个数	矩阵乘法复杂度	算法时间复杂度
Wang et al., 2018[22]	$n(n-1)$	$O(n^3)$	$O(n^3)$
Hua et al., 2022[15]	$n(n-1)/2$	$O(n^3)$	$O(n^3)$
Fan et al., 2022[17]	$n(n-1)$	$O(n^3)$	$O(n^3)$
Liu et al., 2023[18]	$n(n-1)/2$	$O(n^3)$	$O(n^3)$
本文方法	$3n-4$ ($b_i \neq 0$) $2n-4$ ($b_i = 0$)	无	$O(n)$

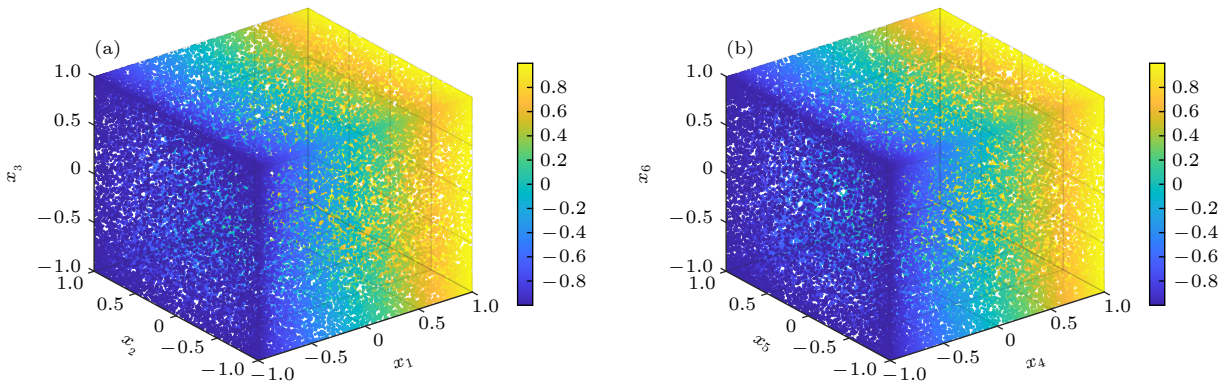

图 1 (a) x_1-x_2-x_3 相图; (b) x_4-x_5-x_6 相图

Fig. 1. (a) x_1-x_2-x_3 phase diagram; (b) x_4-x_5-x_6 phase diagram.

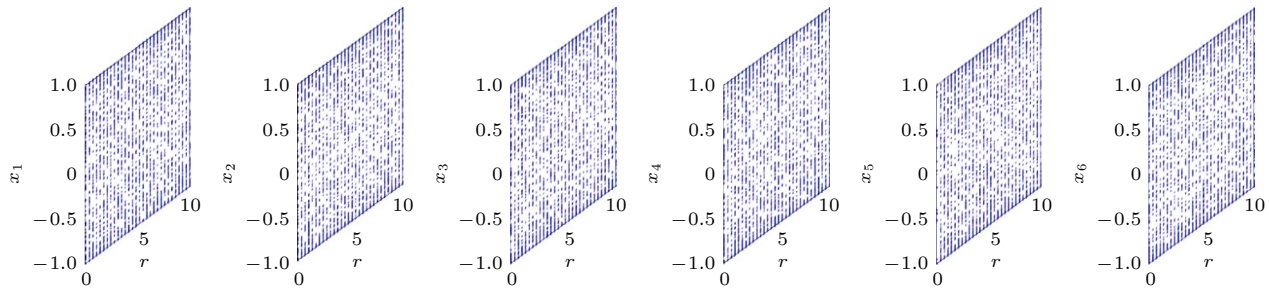

图 2 分岔图

Fig. 2. Bifurcation diagram.

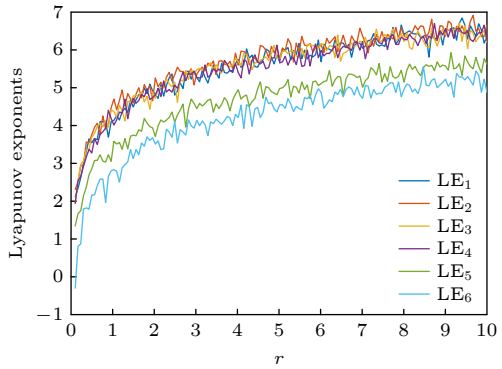

图 3 Lyapunov 指数

Fig. 3. Lyapunov exponent.

3) 熵指标分析

本部分选取多个维度分析了构建的 n 维混沌系统的动力学特征, 选取常见指标来进行评价. KE (Kolmogorov entropy) 通过测试动态系统的信息丢失程度来衡量系统运动的不可预测性 [23]. 正的 KE 值表明需要额外的信息来预测一个动态系统的轨迹, 混沌映射的 KE 越大, 它就越不可预测. SE (sample entropy) 用于测量任何混沌映射生成的时间序列的复杂度 [24]. 样本熵越大, 时间序列越复杂. CD (correlation dimension) 是一种分形维数 [25], 可以测量一组离散状态点所占空间的维数, 由此来判断它的性能以及是否可以应用于加密中. 由表 2 可以看出, 系统在不同维度下的多个指标均表现优秀, 与其他混沌系统对比如表 3 所列, 说明系统是具有复杂动力学行为的超混沌系统.

表 2 不同维度下各个变量动力学指标平均值分析

Table 2. Analysis of average dynamic indicators of variables across different dimensions.

维度	KE	SE	CD
3	0.4312	2.0120	2.1857
4	0.4212	2.0446	2.8712
5	0.4320	2.0973	2.2378
6	0.4226	2.9321	2.7423

表 3 不同 6D 混沌系统的 6 个变量平均值对比

Table 3. Comparison of average values of six variables across different 6D chaotic systems.

系统	CD	SE
Zhao et al., 2023[18]	2.8493	2.0191
Zeng et al., 2023[26]	2.8115	2.2268
Liu et al., 2023[27]	2.8893	2.6958
Xing et al., 2024[28]	1.4833	1.6015
新的混沌系统	2.7423	2.9321

4) TestU01

TestU01 是一款用于测试随机性的工具, 其中包括 8 项测试. 本节使用其中的 3 个测试来测量本文所提系统的随机性. 其中, BigCrush 是强度最大的测试. 表 4 显示了由混沌系统产生的混沌信号的测试结果. 从表 4 可以看出, 所设计的 6D 混沌系统生成的序列能大部分顺利通过 SmallCrush, 但面对更强大的 BigCrush 没有表现出良好的性能, 尤其是最强的 BigCrush, 这是未来工作需要改进的方向.

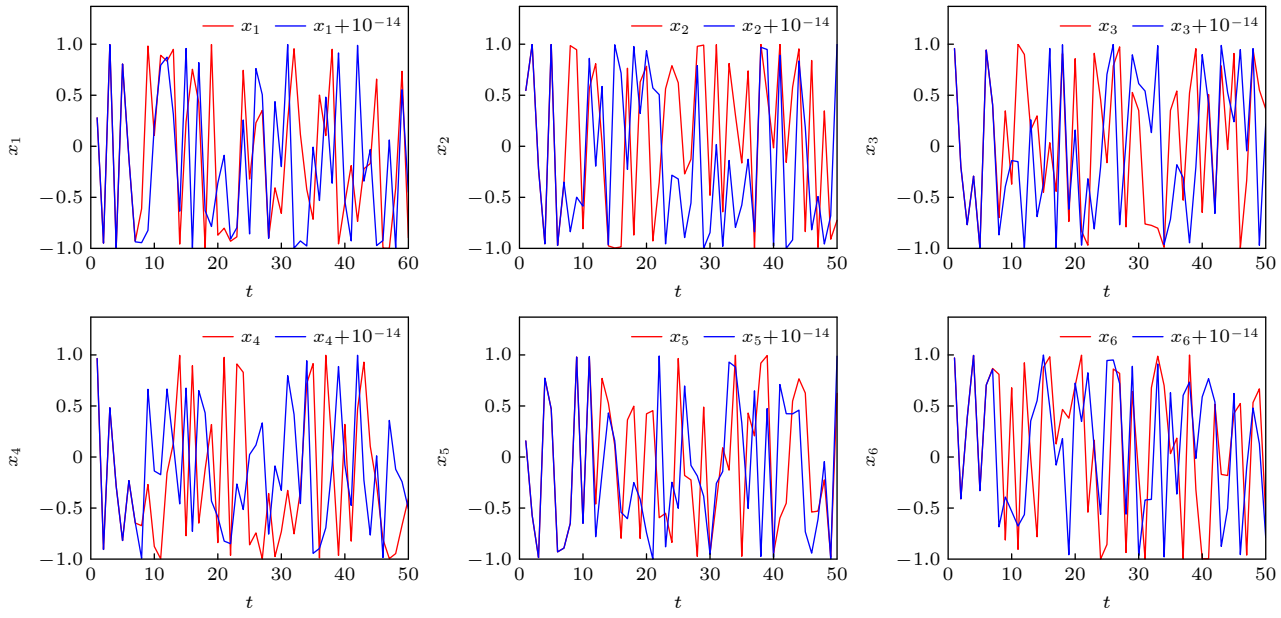

图 4 敏感性分析

Fig. 4. Sensitivity analysis.

表 4 TestU01 测试结果 (未通过的数量)
Table 4. TestU01 test results (number of failures).

变量(增益10^{15})	x_1	x_2	x_3	x_4	x_5	x_6
SmallCrush(15)	0	0	0	0	2	0
Crush(144)	6	4	7	6	78	4

4 音频加密方法

4.1 加密过程

步骤 1 输入明文语音, 使用通过 API 接口从 http://www.random.org/获取的真随机数生成器获取初值 $[x_1,\ x_2,\ x_3,\ x_4,\ x_5,\ x_6]$, 设置系统参数 $r=100$, 新的六维混沌系统产生 6 条混沌序列 $X_1,\ X_2,\ X_3,\ X_4,\ X_5,\ X_6$, 每次加密时都会重新获取全新的真随机数作为下一轮的初始值, 若偶然出现初值重复的情况, 则重新调用该接口确保获得一个不同的初值, 从而实现了一次一密的加密机制.

步骤 2 将语音 P 映射到 $[0,255]$ 得到 P_0, 采用 K-means 算法将 P_0 分为六组得到 $\boldsymbol{P}_1$, 其中 $\boldsymbol{P}_1=[P_{11},\ P_{12},\ P_{13},\ P_{14},\ P_{15},\ P_{16}]$. 使用下面的公式将每个元素映射为 $[0,255]$:

$$P_0=\text{floor}\left(\frac{(P-\min(P))\times 255}{\max(P)-\min(P)}\right). \tag{9}$$

步骤 3 利用产生的混沌序列对语音序列 $\boldsymbol{P}_1$ 进行置乱得到 $\boldsymbol{P}_2=[P_{21},\ P_{22},\ P_{23},\ P_{24},\ P_{25},\ P_{26}]$, $\text{sort}\,(a,L)$ 表示按升序对长度为 L 的序列 a 进行排序, 其具体过程如下:

$$\begin{cases} M_i=\text{lenght}(P_{1i}); \\ [J_i]=\text{sort}(X_1,M_i),\quad i=1,2,3,4,5,6; \\ P_{2i}=P_{1i}(J_i). \end{cases} \tag{10}$$

步骤 4 将混沌序列 X_1 转化为 0 到 255 之间的整数序列 $Y=[Y_1,Y_2]$, 然后按 $\boldsymbol{P}_2$ 的正向进行异或运算, 再按一维向量 $\boldsymbol{P}_2$ 的逆向进行异或运算, 其中 M 为 $\boldsymbol{P}_2$ 的长度, 最终得到密文 C, 其具体过程如下:

$$\begin{cases} B(0)=0,\ B(1)=B(0)\oplus Y_1(1)\oplus P_2(1); \\ B(i)=B(i-1)\oplus Y_1(i)\oplus P_2(i),\ i=2:M; \\ C(0)=0,\ C(M)=C(0)\oplus Y_2(M)\oplus B(M), \\ C(i)=C(i+1)\oplus Y_2(i)\oplus B(i), i=M-1:1. \end{cases} \tag{11}$$

4.2 解密过程

解密过程为加密过程的逆过程, 具体步骤如下:

步骤 1 输入密文语音 C, $r=100$, 密钥 x_1, x_2, x_3, x_4, x_5, x_6 得到混沌序列 $D1$, $D2$, $D3$, $D4$, $D5$, $D6$.

步骤 2 进行正向扩散和逆向扩散的逆过程, 操作得到 $\boldsymbol{P}_2$.

步骤 3 进行位置置乱算法逆算法得到 $\boldsymbol{P}_1$.

步骤 4 进行 K-means 逆算法得到 P_0.

步骤 5 将 P_0 映射到原范围得到明文 P.

5 音频加密仿真实验与安全性分析

5.1 仿真结果

在本部分中我们对一些不同的音频数据进行了加密和解密实验, 从图 5 可以看出, 经过加密后明文音频变成了无法识别出有用信息的密文, 再经过解密操作, 可以还原明文, 这说明本文算法能够进行有效的加密与解密.

5.2 安全性分析

1) 相邻像素的相关性分析

我们使用从加密前后的音频中随机选取的一组相邻像素值计算相关系数. 实验结果如表 5 和表 6 所列, 其中 A_n, A_{n+1} 和 A_{n+1} 分别表示该音频的第 n 个, 第 n+1 个, 第 n+2 个元素, 可以看出原文音频的相关性很强, 但是经过我们的算法加密后, 密文的相关系数接近 0, 说明相邻元素具有较

表 5 原始音频相关系数
Table 5. Correlation coefficients of original audio files.

音频	明文		
	A_n, A_{n+1}	A_n, A_{n+2}	A_n, A_{n+3}
1-67152-A-17.wav	0.8980	0.6885	0.5066
1-121951-A-8.wav	0.9695	0.8840	0.7583
5-261464-A-23.wav	0.9559	0.8041	0.6811
平均	0.9411	0.7922	0.6487

表 6 加密音频相关系数
Table 6. Correlation coefficients of encrypted audio files.

音频	密文		
	A_n, A_{n+1}	A_n, A_{n+2}	A_n, A_{n+3}
1-67152-A-17.wav	–0.0029	–0.0036	0.0011
1-121951-A-8.wav	–0.0017	0.0017	–0.0013
5-261464-A-23.wav	0.0020	0.0019	0.0027
绝对值平均	0.0022	0.0024	0.0017

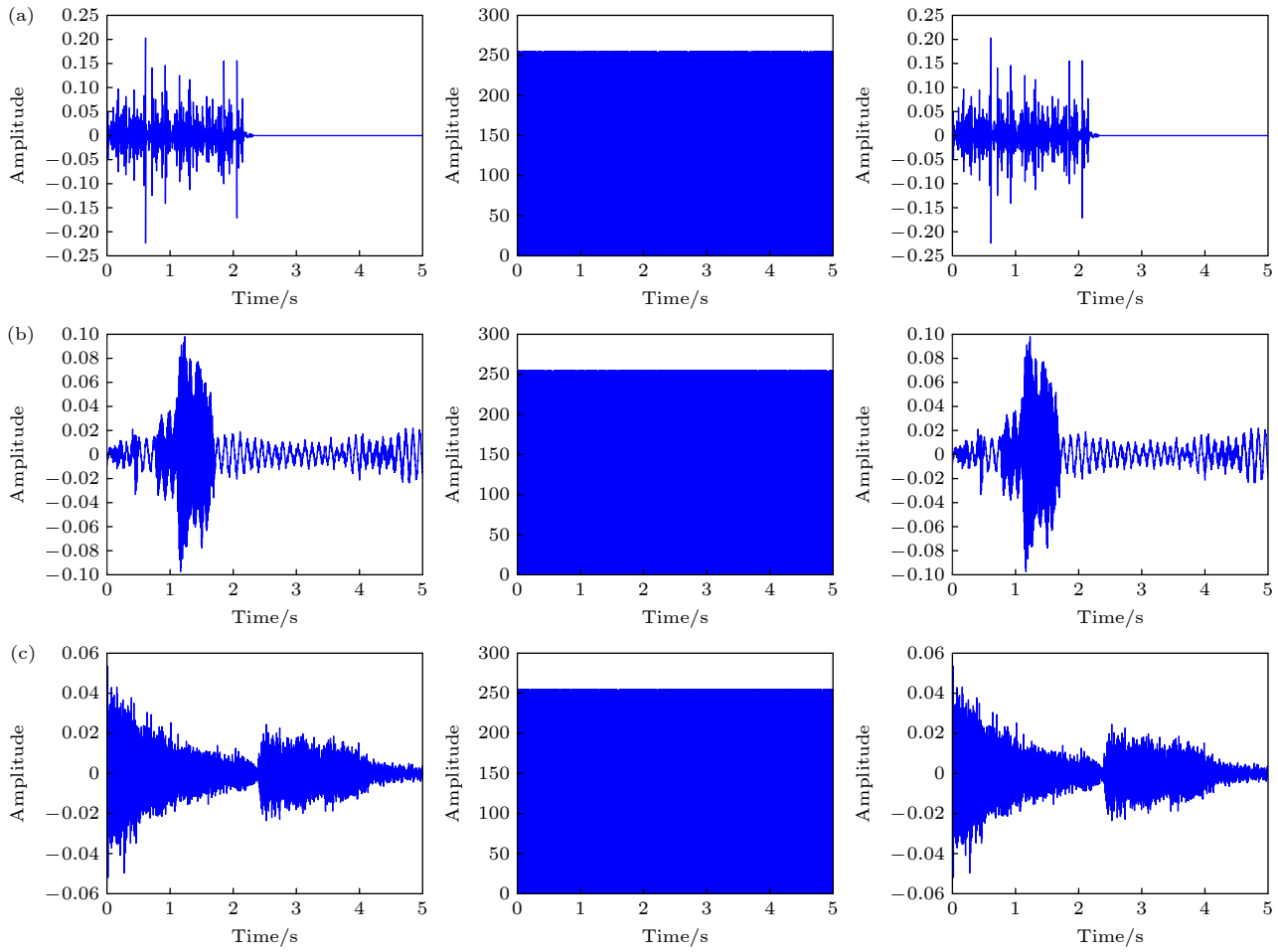

图 5 音频加密与解密仿真 (第 1 列为原始音频波形图; 第 2 列为加密音频波形图; 第 3 列为解密音频波形图) (a) 1-67152-A-17.wav 的加密与解密; (b) 1-121951-A-8.wav 的加密与解密; (c) 5-261464-A-23.wav 的加密与解密

Fig. 5. Audio encryption and decryption simulation (the first column is the original audio waveform diagram; the second column is an encrypted audio waveform diagram; the third column decrypts the audio waveform diagram): (a) Encryption and decryption of 1-67152-A-17.wav; (b) encryption and decryption of 1-121951-A-8.wav; (c) encryption and decryption of 5-261464-A-23.wav.

表 7 加密音频相关系数对比

Table 7. Comparison of correlation coefficients of encrypted audio files.

算法	本文	Rahul et al., 2023[6]	Kumar et al., 2023[29]	Cao et al., 2024[9]	Wu et al., 2024[5]
相关系数	0.0022	0.000013	0.0019	0.002512	0.0013

小的相关性. 表 7 展示了与多种算法的密文相关系数的对比结果. 可以看出, 本算法加密得到的密文相关系数与其他方法一样接近于零, 这表明该算法完全能够抵抗统计攻击.

2) 选择明文攻击

我们选取 3 个音频文件, 然后任意两个音频文件进行组合, 通过使用公式

$$\mathrm{NSCR}=\frac{1}{L}\sum_{i=1}^{L}|\mathrm{sign}(\lfloor C_1(i)\rfloor-\lfloor C_2(i)\rfloor)|\times 100\%$$

来衡量明文和明文以及密文和密文之间的差异[4], 其中 C_1 为原始密文, C_2 为新密文. 图 6(a)—6(c) 表示任意两类明文异或的结果图, 而图 6(d)—(f) 表示两个明文分别对应两个密文异或的结果图. 图 6(a) 中的音频与图 6(d) 中的音频之间的 NSCR 为 99.61%, 图 6(b)中的音频与图 6(e) 中的音频之间的 NPCR 为 99.63%, 图 6(c) 中的音频与图 6(f) 中的音频之间的 NSCR 为 99.61%. 很明显, $\lfloor A_1(i,j)\rfloor\oplus\lfloor A_2(i,j)\rfloor\neq\lfloor C_1(i,j)\rfloor\oplus\lfloor C_2(i,j)\rfloor$. 因此, 本算法可以抵御选择明文攻击.

3) 信息熵分析

表 8 显示了加密音频信息和原始音频信息的信息熵. 由于将音频转化为 0—255 之间的整数, 故该算法加密后的语音信息熵接近 8, 说明该算法可以抵抗统计攻击.

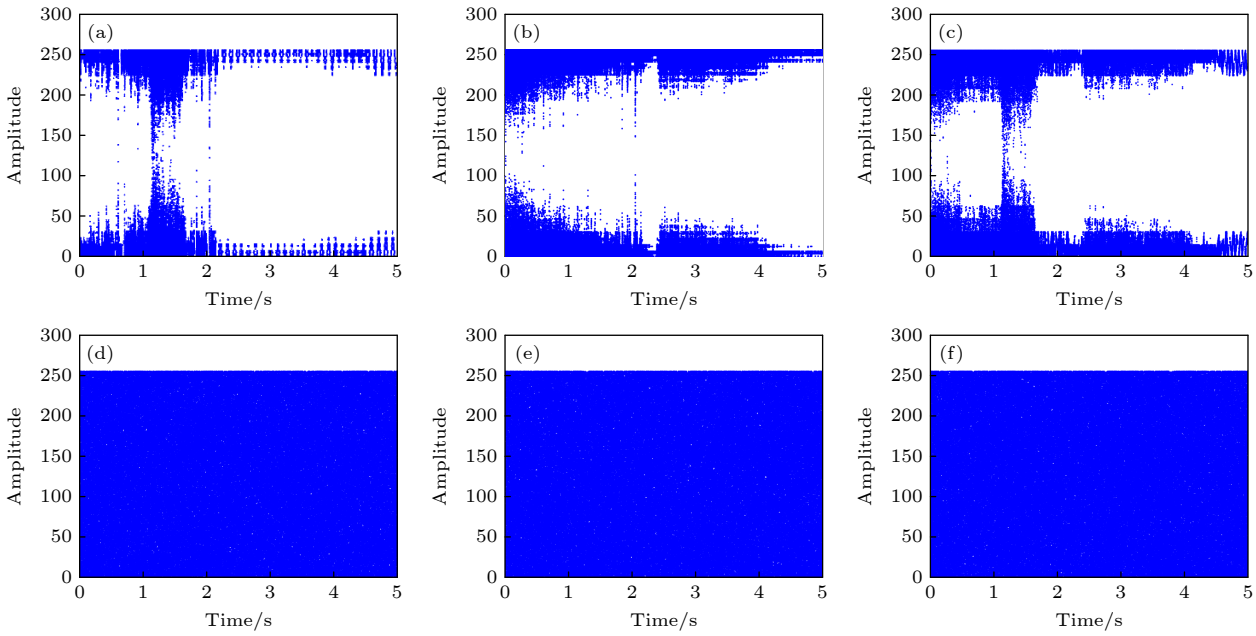

图 6 选择明文攻击 (a) 1-67152-A-17.wav XOR 1-121951-A-8.wav; (b) 5-261464-A-23.wav XOR 1-67152-A-17.wav; (c) 1-121951-A-8.wav XOR 5-261464-A-23.wav; (d) 加密后的 1-67152-A-17.wav XOR 加密后的 1-121951-A-8.wav; (e) 加密后的 5-261464-A-23.wav XOR 加密后的 1-67152-A-17.wav; (f) 加密后的 1-121951-A-8.wav XOR 加密后的 5-261464-A-23.wav

Fig. 6. Chosen-plaintext attack: (a) 1-67152-A-17.wav XOR 1-121951-A-8.wav; (b) 5-261464-A-23.wav XOR 1-67152-A-17.wav; (c) 1-121951-A-8.wav XOR 5-261464-A-23.wav; (d) encrypted 1-67152-A-17.wav XOR encrypted 1-121951-A-8.wav; (e) Encrypted 5-261464-A-23.wav XOR Encrypted 1-67152-A-17.wav; (f) encrypted 1-121951-A-8.wav XOR encrypted 5-261464-A-23.wav.

表 8 加密音频的信息熵

Table 8. Information entropy of encrypted audio files.

音频	明文	密文
1-67152-A-17.wav	1.0577	7.9993
1-121951-A-8.wav	1.9480	7.9993
5-261464-A-23.wav	1.3021	7.9993
平均	1.4359	7.9993

表 9 加密效率

Table 9. Encryption efficiency.

音频	大小	加密时间/s	速度/(s·KB^{-1})
1-67152-A-17.wav	430	0.2809	0.00065
1-121951-A-8.wav	430	0.2097	0.00048
5-261464-A-23.wav	430	0.2167	0.00050
平均	430	0.2357	0.00054

表 10 加密效率对比

Table 10. Comparison of encryption efficiency.

算法	本文算法	Wu et al., 2024[5]	Joshi et al., 2024[2]	Kumar et al., 2023[29]
速度/(s·KB^{-1})	0.00054	0.00030	1.8309	0.0041

4) 效率分析

接下来分析该算法的加密时间和效率. 表 9 展示了本加密算法的加密时间和加密效率. 从表 10 可看出, 对比 Kumar 与 Dua[29] 和 Joshi 与 Gaffar[2] 的平均效率, 本算法耗时短, 加密效率大大提高. 与 Wu 等[5] 对比, 本算法与它的加密效率差不多. 综上, 可以说明本文算法具有较高的加密效率.

5) 密钥空间分析

本文算法得密钥空间包含 x_1, x_2, x_3, x_4, x_5, x_6, r, 其中, $x_1, x_2, x_3, x_4, x_5, x_6$ 为系统的初值, r 为系统的参数. 假设计算机的精度为 10^{-14}, 相应的密钥空间大小为 $10^{14\times7} \approx 2^{325} > 2^{100}$, 这表示新的音频加密算法具有抗穷举攻击能力.

6 结 论

本文主要提出一种具有全局有界的 nD($n \geqslant 3$) 并且具有 n 个正 Lyapunov 的超混沌系统, 该系统通过正弦函数可以生成具有所需动态特性的 n 维混沌映射. 该系统因涉及较少的项数和运算量而具有简单的结构, 并通过动力学分析揭示出其具有连续的混沌区间. 与其他一些系统相比, 它展现出更高的复杂性和分形维数. 最后, 以 6D 为实例结合

前后项异或算法与真随机数设计新的音频加密算法. 仿真结果表明, 与其他方法相比, 该算法既可以满足各种统计测试, 也可以实现一次一密, 具有较高安全性. 这也验证了所构建的超混沌系统可以有效的应用在音频加密领域.

参考文献

[1] Herbadji D, Herbadji A, haddad I, Kahia H, Belmeguenai A, Derouiche N 2024 *Integration* **97** 102192
[2] Joshi A B, Gaffar A 2024 *Soft Comput.* **28** 5523
[3] Yu F, Yu Q L, Chen H F, Kong X X, Molbel A A M, Cai S, Du S C 2022 *Fractal Fract.* **6** 370
[4] Wu R, Gao S, Wang X Y, Liu S B, Li Q, Erkan U, Tang X L 2022 *Chaos, Soliton Fractals* **165** 112770
[5] Wu R, Gao S, Iu H H, Zhou S, Erkan U, Toktas A, Tang X 2024 *IEEE Internet Things J.* **11** 10214
[6] Rahul B, Kuppusamy K, Senthilrajan A 2023 *Multimed. Tools Appl.* **82** 43729
[7] Demirtaş M 2023 *Orclever Proc. Res. Dev.* **2** 28
[8] Liu H J 2023 *Multimed. Tools Appl.* **82** 27973
[9] Cao Y F, Liu H J 2024 *Multimed. Tools Appl.* **83** 79377
[10] Zhu P X, Yang Q G 2023 *Proc. Am. Math. Soc.* **151** 5353
[11] Wang X Y, Wang M J 2007 *Acta Phys. Sin.* **56** 6843 (in Chinese) [王兴元, 王明军 2007 物理学报 **56** 6843]
[12] Yang Q G, Zhu P X 2024 *Int. J. Bifurcation Chaos* **34** 2450122
[13] Zhao Z P, Zhou S, Wang X Y 2021 *Acta Phys. Sin.* **70** 230502 (in Chinese) [赵智鹏, 周双, 王兴元 2021 物理学报 **70** 230502]
[14] Fu L X, He S B, Wang H H, Sun K H 2022 *Acta Phys. Sin.* **71** 030501 (in Chinese) [扶龙香, 贺少波, 王会海, 孙克辉 2022 物理学报 **71** 030501]
[15] Hua Z Y, Zhang Y X, Bao H, Huang H J, Zhou Y C 2022 *IEEE Trans. Circuits Syst. Regul. Pap.* **69** 784
[16] Huang L L, Liu J, Xiang J H, Zhang Z F, Du X L 2022 *Chaos, Soliton Fractals* **160** 112248
[17] Fan C L, Ding Q 2022 *Chaos, Soliton Fractals* **161** 112323
[18] Zhao M D, Liu H J 2023 *Int. J. Bifurcation Chaos* **33** 2350070
[19] Zhang Y X, Hua Z Y, Bao H, Huang H J, Zhou Y C 2023 *IEEE Trans. Syst. Man Cybern Syst.* **53** 6516
[20] Ding D W, Zhu H F, Zhang H W, Yang Z L, Xie D 2024 *Chaos, Soliton Fractals* **185** 115168
[21] MacQueen J 1967 *Proceedings of the 5th Berkeley Symposium on Mathematical Statistics and Probability*, USA, June 21–July 18 1965 and December 27, 1965–January 7, 1966 p281
[22] Wang C F, Fan C L, Ding Q 2018 *Int. J. Bifurcation Chaos* **28** 1850084
[23] Termonia Y 1984 *Phys. Rev. A* **29** 1612
[24] Richman J S, Moorman J R 2000 *Am. J. Physiol-Heart C* **278** H2039
[25] Grassberger P, Procaccia I 1983 *Phys. Rev. Lett.* **50** 346
[26] Zeng J, Wang Y M, Li X Y, Guang Y R, Wang C F, Ding Q 2023 *Phys. Scr.* **98** 075212
[27] Liu R R, Liu H J, Zhao M D 2023 *Integration* **93** 102071
[28] Xing Y N, Zeng J, Dong W J, Zhang J, Guo P T, Ding Q 2024 *Phys. Scr.* **99** 035231
[29] Kumar A, Dua M 2023 *Appl. Acoust.* **203** 109196

An n-dimensional discrete hyperchaotic system and its application in audio encryption*

Zhou Shuang[1)†] Yin Yan-Li[1)] Wang Shi-Yu[1)] Zhang Ying-Qian[2)3)]

1) (*School of Mathematical Sciences, Chongqing Normal University, Chongqing* 401331, *China*)

2) (*Xiamen University Tan Kah Kee College, Zhangzhou* 363105, *China*)

3) (*Xiamen University Malaysia, Sepang*, 43900, *Malaysia*)

(Received 24 July 2024; revised manuscript received 26 August 2024)

Abstract

Discrete chaotic system, as a pseudo-random signal source, plays a very important role in realizing secure communication. However, many low-dimensional chaotic systems are prone to chaos degradation. Therefore, many scholars have studied the construction of high-dimensional chaotic systems. However, many existing algorithms for constructing high-dimensional chaotic systems have relatively high time complexity and relatively complex structures. To solve this problem, this paper explores an n-dimensional discrete hyperchaotic system with a simple structure. Firstly, the n-dimensional discrete hyperchaotic system is constructed by using sine function and power function and simple operations. Then, it is theoretically analyzed based on Jacobian matrix method that the system can have the positive Lyapunov exponents. Next, the algorithm time complexity, sample entropy, correlation dimension and other indexes are compared with those of the existing methods. The experimental results show that our system has a simple structure, high complexity and good algorithm time complexity. Therewith, a six-dimensional chaotic system is chosen as an example, and the phase diagram, bifurcation diagram, Lyapunov expnonents, complexity and other characteristics of the system are analyzed. The results show that the proposed system has good chaotic characteristics. Moreover, to show the application of the proposed system, we apply it to audio encryption. According to this system, we combine it with the XOR operation and true random numbers to explore a novel method of one-cipher audio encryption. Through experimental simulation, compared with some existing audio encryption algorithms, this algorithm can satisfy various statistical tests and resist various common attacks. It is also validated that the proposed system can be effectively applied to the field of audio encryption.

Keywords: discrete hyperchaotic system, Lyapunov exponent, audio encryption, K-means algorithm

PACS: 05.45.Pq, 05.45.Vx **DOI:** 10.7498/aps.73.20241028

CSTR: 32037.14.aps.73.20241028

* Project supported by the Natural Science Foundation Project of Chongqing, China (Grant No. CSTB2023NSCQ-MSX0401).

† Corresponding author. E-mail: zhoushuang@cqnu.edu.cn

物理学报 Acta Physica Sinica
Chinese Physical Society
Institute of Physics, CAS

*n*维离散超混沌系统及其在音频加密中的应用

周双 尹彦力 王诗雨 张盈谦

An *n*–dimensional discrete hyperchaotic system and its application in audio encryption

Zhou Shuang Yin Yan-Li Wang Shi-Yu Zhang Ying-Qian

引用信息 Citation: Acta Physica Sinica, 73, 210501 (2024) DOI: 10.7498/aps.73.20241028
在线阅读 View online: https://doi.org/10.7498/aps.73.20241028
当期内容 View table of contents: http://wulixb.iphy.ac.cn
