文章编号：2095-2163(2022)03-0053-08 中图分类号：TP309.7 文献标志码：A

基于改进 3D-Hénon 混沌映射的音频加密算法研究

妥永强，巫朝霞
（新疆财经大学 统计与数据科学学院，乌鲁木齐 830012）

摘 要：针对低维 Hénon 映射混沌在加密时存在混沌空间小、安全性低等问题，提出了改进的 3D-Hénon 混沌映射音频加密算法。首先通过对二维 Hénon 混沌映射进行升维与改进，得到改进的 3D-Hénon 混沌映射，并与离散化的超混沌系统结合，生成伪随机序列；通过 NIST sp800_22 测试检验序列随机性，将秘钥与明文音频互相关联，实现了“一次一密”，降低了选择明文攻击的可能性；利用生成的伪随机序列进行循环排序置乱，以及向前向后扩散完成加密。通过仿真与抗攻击性实验表明，本文提出的音频加密算法具有较强的秘钥敏感性和足够大的秘钥空间，相邻振幅间相关性较低，与明文音频的峰值信噪比较低，该算法具有良好的抗统计攻击性以及鲁棒性。

关键词：音频加密；峰值信噪比；鲁棒性；循环排序置乱

Research on audio encryption algorithm based on improved 3D-Hénon chaos map

TUO Yongqiang, WU Zhaoxia
(School of Statistics and Data Science, Xinjiang University of Finance and Economics, Urumqi 830012, China)

【Abstract】 Aiming at the problems of small chaotic space and low security in the encryption of low-dimensional Hénon map chaos, an improved audio encryption algorithm based on 3D-Hénon chaotic map is proposed. The pseudo-random sequence generated by the Hénon chaotic map combined with the discretized hyper-chaotic system, and the randomness of the sequence is verified by the NIST sp800_22 randomness test, and the secret key and the plaintext audio are correlated to each other. Select the possibility of plaintext attack, use the generated pseudo-random sequence to perform circular sorting scrambling and forward and backward diffusion to complete encryption. Simulation and anti-attack performance experiments show that the proposed audio encryption algorithm has strong key sensitivity and The key space is large enough, the correlation between adjacent amplitudes is low, and the peak signal-to-noise ratio of plaintext audio is low. The encryption algorithm has good resistance to statistical attacks and robustness.

【Key words】 audio encryption; peak signal to noise ratio; robustness; circular sort scrambling

0 引 言

21 世纪以来，信息成为日趋重要的生产要素。互联网具有无穷的信息获取与简易的信息交换机能，网络的全球化也使得信息的索取、传递与交换更加便捷。如今，网络化信息已渗透于社会生活的方方面面，在经济、政治、艺术和科学等领域应用广泛。于此同时，人们对信息隐私安全也提出了更高的要求，信息隐私安全受到了严峻的挑战。传统的加密技术只适用于文本加密，不适用于数据量大、冗余度高的音频加密[1]，所以寻求高质量的音频加密技术具有重大的研究意义。

近年来，由于混沌系统表现出优良的初值敏感性、遍历性以及不确定性，国内外许多学者将其广泛运用于图像加密以及音频加密领域。如：文献[2]中将 Arnold 映射扩展至 N 维空间后得到高维混沌映射，从而构建了混沌查找表，使用密码区块链模式将其应用于音频加密。但该算法实现难度较高，具有一定的局限性。文献[3]利用 Logistic 混沌映射构建映射关系进行音频的置乱加密。该算法虽然降低了复杂性，但秘钥空间较小，抵抗统计攻击性能较差，易被破解。针对上述问题，文献[4]中设计了基于多涡卷混沌系统的音频加密算法。该算法的初始秘钥同时取决于音频的 Hash 值和外部密钥，在增加秘钥空间的同时，有效提高了选择明文攻击与统计攻击的难度。文献[5]利用随机矩阵对音频信号进行扩充后，通过 Logistic 混沌映射，分别在时域、小波域、时域对音频进行加密。文献[6]利用细胞神经网络混沌与 Logistic 混沌映射构造出多级秘钥后，通过 Logistic 混沌映射对音频进行加密。

基金项目：国家自然科学基金(61941205)。

作者简介：妥永强(1996-)，男，硕士研究生，主要研究方向：信息安全；巫朝霞(1975-)，女，博士，教授，主要研究方向：信息安全。

通讯作者：巫朝霞 Emial：wuzhaoxia828@163.com

收稿日期：2022-01-04

本文在上述研究的基础上,提出了一种将改进的 3D-Hénon 混沌映射与离散化超混沌系统相结合的多混沌音频加密算法,并给出了仿真实验结果以及安全性能分析。

1 混沌系统

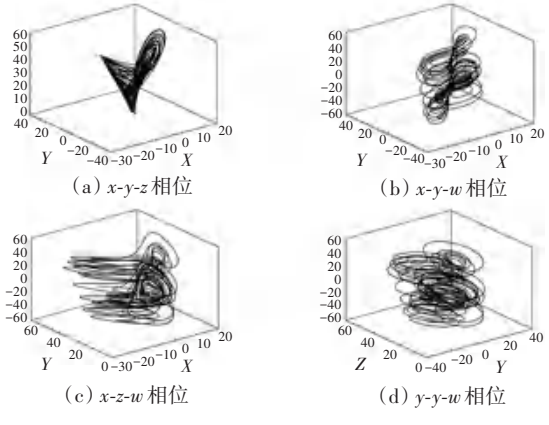
定义 1 超混沌 Chen 系统

4 维超混沌 Chen 系统[7],其定义如式(1):

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x + y - xz + \omega \\ \dot{z} = xy - bz \\ \dot{\omega} = kyz \end{cases} \tag{1}$$

其中, $a = 10; b = -8/3; c = 38$; k 是一个 0 ~ 1 之间的参数。

本文选取 $k = 0.02$,此时系统的 4 个 Lyapunov 指数分别为:0.969,0.042,-12.67,0。其中有两个正指数,说明该系统是超混沌系统。使用四阶 Runge-Kutta 算法对式(1)离散化(时间间隔 $T = 0.02$),得到超混沌 Chen 系统部分相图如图 1 所示。



(a) x-y-z 相位 (b) x-y-w 相位 (c) x-z-w 相位 (d) y-y-w 相位

图 1 超混沌 Chen 系统吸引子相位图

Fig. 1 Attractor phase diagram of hyperchaotic Chen system

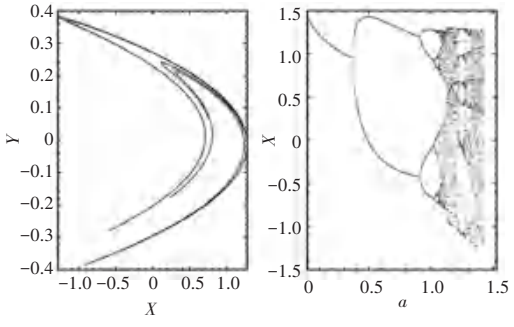
定义 2 改进的 3D-Hénon 映射混沌系统

1976 年,法兰西数学家 Hénon 受 Pomeau 关于洛伦兹系统数值结果的启发,通过对 (x,y) 平面自身的 3 个映射链来模拟,并调节参数得出的二维映射,作为一种简单的高维混沌映射,具有优良的非线性动力学特征,其定义如式(2):

$$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \tag{2}$$

其中, a、b 为二维 Hénon 混沌映射的控制参数。

图 2 为参数 $b = 0.3$,初始值为 $x_0 = 0.15, y_0 = 0.25$时的 Hénon 混沌映射混沌轨道图及分岔图。通过分岔图可得出:当参数 $1.06 < a < 1.22$ 或 $1.27 < a < 1.29$ 或 $1.31 < a < 1.42$ 范围内时,其处于混沌状态,系统有正的最大 Lyapunov 指数。



(a) 轨道图 (b) 分岔图

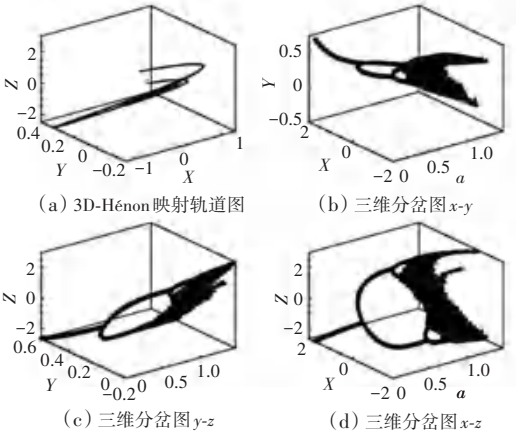
图 2 Hénon 映射的序列轨道图与分岔图(a=1.4)

Fig. 2 Sequence track and bifurcation diagrams of Hénon mapping

通过对式(2)进行调整及改进,添加变量 z 及控制参数 c、d,得到改进的 3D-Hénon 映射。其定义如式(3):

$$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2 \\ y_{n+1} = bx_n - cy_nz_n \\ z_{n+1} = y_n - dx_n \end{cases} \tag{3}$$

其中, a、b、c、d 为 3D-Hénon 映射的控制参数($b = 0.3, c = 0.1, d = 2$)。图 3 为初始值为 $x_0 = 0.2$, $y_0 = 0.1, z_0 = 0.3$ 时改进的 3D-Hénon 混沌映射混沌轨道及三维分岔图。同样,当参数 $1.06 < a < 1.22$ 或 $1.27 < a < 1.29$ 或 $1.31 < a < 1.42$ 范围内时,处于混沌状态,系统有正的最大 Lyapunov 指数。



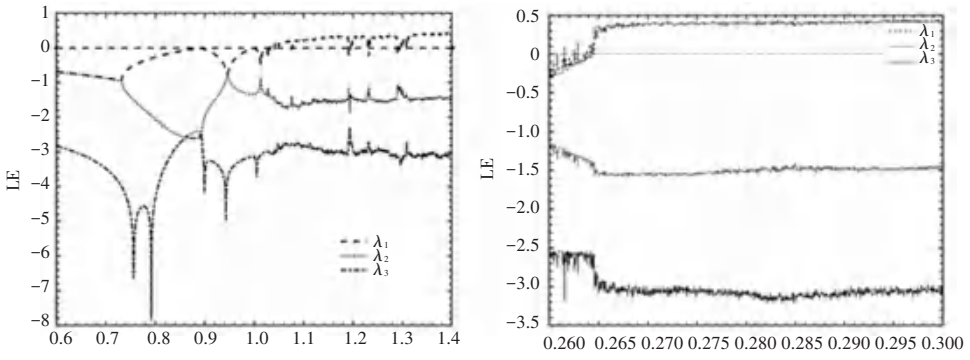
(a) 3D-Hénon映射轨道图 (b) 三维分岔图x-y (c) 三维分岔图y-z (d) 三维分岔图x-z

图 3 改进 3D-Hénon 映射的序列轨道图与三维分岔图

Fig. 3 Improved 3D Hénon map sequence orbit diagram and 3D bifurcation diagram

Lyapunov 指数是利用数值方法描述非线性动力学系统稳定性的一种重要方法,是衡量非线性动力学系统在其相空间中沿某方向运动过程中各轨道之间相互靠近与远离的一种指数级度量,提供了混沌系统动力学行为的定性和定量特征。当非线性动力

学系统为离散映射系统时，若最大 Lyapunov 指数为正时，其具有混沌行为。图 4 为改进的 3D−Hénon 映射在控制参数 a、b 变化时，$c = 0.1$，$d = 2$，初始值 $x_0 = 0.2$，$y_0 = 0.1$，$z_0 = 0.3$ 时的 Lyapunov 指数图。



（a）参数 a 变化的 Lyapunov 指数　　（b）参数 b 变化的 Lyapunov 指数

图 4　改进 3D−Hénon 映射当参数变化的 Lyapunov 指数图

Fig. 4　Lyapunov exponent plot for improved 3D−Hénon mapping when parameters a and b vary

由图 4 可以看出，当参数 $1.06 < a < 1.22$ 或 $1.27 < a < 1.29$ 或 $1.31 < a < 1.42$ 范围内时，其最大 Lyapunov 指数大于 0，系统处于混沌状态。当参数 $a = 1.4$，$0.265 < b < 0.3$ 时，最大 Lyapunov 指数恒为正，其对参数 b 具有鲁棒性，该混沌系统适合产生用于音频加密的随机数。

2　加密算法设计

2.1　音频预处理

取时长 m 秒的音频进行采样率为 fs(Hz) 的采样后得到 $w(i)$ $(i = 1,2,\cdots,N)$，作为明文音频的音频数据。对音频信号进行分块处理步长为 fs，超出部分用 0 填充，则原始音频信号被分为 m 或 $m + 1$ 块。设 $a(i)$，$(i = 1,2,\cdots,fs)$ 为原始音频信号分块中的一块，分离左右声道 $a_R(i)$ 与 $a_L(i)$。将音频信号振幅放大后，进行坐标系偏移，取整得到增强后的信号序列 $\alpha_R(i)$，$\alpha_L(i)$。

2.2　密钥的选取与生成

(1)用户任意选取 3 个 0~1 之间的数值作为初始密钥 $key0 = (x_0, y_0, z_0)$；

(2)将初始密钥 $key0$ 作为初始值输入改进的 3D−Hénon 映射，预迭代系统 t 次，以消除其暂态效应，增强系统初值敏感性。继续迭代 N_0 次生成随机序列：

$$\begin{cases} s_1(i) = x(t+i), (i = 1,2,\cdots,N_0) \\ s_2(i) = y(t+i), (i = 1,2,\cdots,N_0) \\ s_3(i) = z(t+i), (i = 1,2,\cdots,N_0) \end{cases} \tag{4}$$

(3)将向量(5)作为二级密钥：

$$key1 = \begin{pmatrix} s_1(N_0 - \mathrm{mod}(floor(kMVx_0), N_0)) \\ s_2(N_0 - \mathrm{mod}(floor(kMVy_0), N_0)) \\ s_3(N_0 - \mathrm{mod}(floor(kMVz_0), N_0)) \\ M + V \end{pmatrix} \tag{5}$$

其中：$M = \left| \mathrm{mod}\left(\frac{1}{N} \sum_{i=1}^{N} A(i), 0.5 \right) \right|$；

$$V = \left| \mathrm{mod}\left(\frac{1}{N-1} \sum_{i=1}^{N} A(i) - \frac{1}{N} \sum_{i=1}^{N} A(i), 0.5 \right) \right|;$$

mod( ) 为取余函数；k 为足够大的正整数。

2.3　随机数发生器

将二级密钥 $key1$ 作为四维超混沌 Chen 系统的初值，使用四阶 Runge−Kutta 算法(时间间隔 $T = 0.02$)预迭代系统 t 次，以消除其暂态效应，增强系统初值敏感性，截断后继续迭代 fs 次，生成随机序列。在生成序列过程中，每生成 200 个序列，则进行如下扰动，以消除计算机的有限字长效应，通过式 $S_i(j) = x_i(j) + 0.02 \sum_{k=1;k\neq i}^{4} \sin(x_k(j))$，$i = 1,2,3,4$ 生成序列 S_1, S_2, S_3, S_4。对序列做如下处理，用于后续的置乱和扩散。

$$\begin{cases} F_i(j) = floor(\mathrm{mod}(s_i(j) * 10^{14}, fs)) + 1, i = 1,2 \\ D(j) = floor(\mathrm{mod}(s_i(j) * 10^{14}, 2^8 - 1), i = 1,2,3,4 \end{cases} \tag{5}$$

表 1 为伪随机序列的 NIST sp800_22 随机性测试结果。可以看出，待测试序列的 P_v 值均大于 0.01全部通过测试。可以认为文中序列是随机序列，适合作为后续加密过程的加密密码。

表 1 NIST sp800_22 随机性测试结果

Tab. 1 Randomness test results of NIST SP800 22

测试名称	P_v	结果
单比特频率测试	0.511 8	通过
块内频率测试	0.685 0	通过
游程测试	0.175 2	通过
块内最长 1 游程测试	0.208 6	通过
二进制矩阵秩测试	0.156 2	通过
离散傅里叶(谱)测试	0.926 9	通过
非重叠模板匹配测试	0.074 5	通过
重叠模板匹配测试	0.925 5	通过
Maurer 通用统计测试	0.499 9	通过
线性复杂度测试	0.363 0	通过
序列测试	0.013 8	通过
近似熵测试	0.308 7	通过
累加和测试	0.866 2	通过
随机旅行测试	0.664 4	通过
随机旅行变种测试	0.616 2	通过

2.4 循环排序置乱算法

将序列 $F_i(i = 1,2)$ 中的每个序列对 3、7 取余，分别提取余数为 0 的序列和剩余序列，按照“先升序后降序”的规则进行排序，得到 6 条索引序列 In_i，$(i = 1,\cdots,6)$。将 6 个索引序列进行分组，定义如下规则，得到新索引序列：$index_i = [\varepsilon_i \quad \beta_i \quad \delta_i]$。

其中：

$$\begin{cases} \varepsilon_i = In_i \\ \beta_i = g(In_i, In_{2i}) + In_{2i} \\ \delta_i = g(g(In_i, In_{2i}) + In_{2i}, In_{3i}) + In_{3i} \\ g(\Phi, \Gamma) = \max(\Phi) \times \boldsymbol{ones}(1, \max(\Gamma)) \end{cases} \quad (i = 1,2) \tag{6}$$

$\boldsymbol{ones}(A,B)$ 表示 A 行 B 列的全 1 矩阵。

分别对序列 $\alpha_{NR}(i)$、$\alpha_{NL}(i)$ 进行置乱。置乱时每个元素依次循环索引序列的初始位置、1/3 位置、2/3 位置处置乱。置乱规则，是将 $a(i)$ 元素与 $a(\text{index}(i))$ $(i = 1,2,\cdots,fs)$ 元素调换位置。分别对所有序列置乱后，得到置乱音频序列 $\alpha_{ZNR}(i)$、$\alpha_{ZNL}(i)$。

2.5 扩散算法

对置乱后的序列进行向前扩散与向后扩散。扩散规则如下：

$$\begin{cases} B_1(i) = ((((B_1(i-1) \oplus D_1) \oplus \alpha(i)) \oplus D_2) \oplus \alpha(i-1)) \\ C_1(i) = ((((C_1(i-1) \oplus D_3) \oplus B_1(i)) \oplus D_4) \oplus B_1(i-1)) \end{cases} \tag{7}$$

通过式(7)对置乱音频扩散得到加密音频序列 C_R、C_L，合并后得到加密后的音频。音频加密流程如图 5 所示：

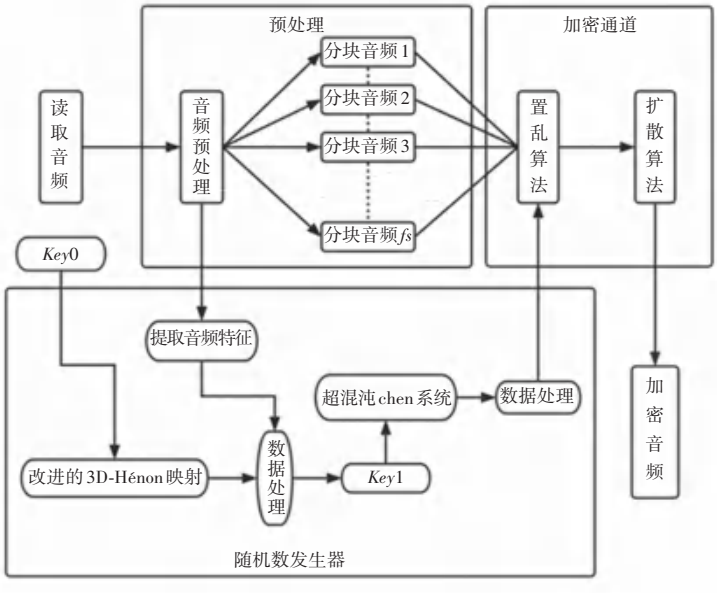


图 5 音频加密流程图

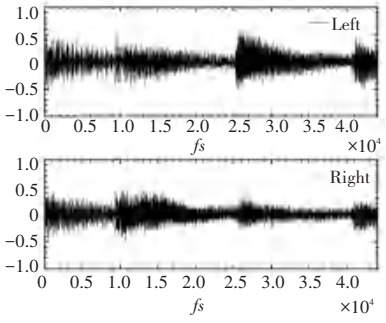
Fig. 5 Flow chart of Audio encryption

3　实验仿真与性能分析

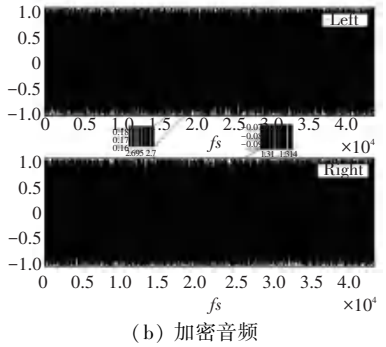
3.1　实验仿真

实验仿真采用双声道音频“Audio1.wav”，分别截取其中一块进行实验仿真。实验参数分别设置为：$k = 2^{14}$，$N_0 = 30\,000$，$t = 8\,000$，$key0 = (0.141\,592\,6, 0.653\,589)$，$key1 = (0.969\,015, 0.409\,086, 0.622\,289, 0.640\,965)$。

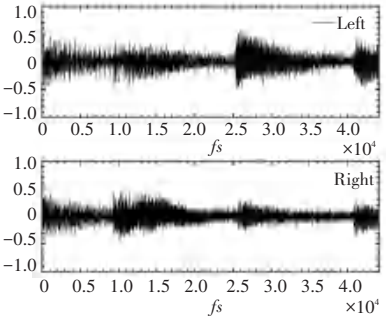
图 6(a)~6(c)分别为原始音频波形图、加密音频波形图、解密音频波形图。可以看出，加密后的音频波形图呈现无规则杂乱状，已与原始音频无任何关联，经解密后的音频波形图与原始音频波形图完全相同。



(a) 原始音频



(b) 加密音频



(c) 解密音频

图 6　音频加密仿真实验结果

Fig. 6　Audio encryption simulation results

3.2　密钥敏感性与密钥空间分析

相对于原始秘钥，一个细微差别的密钥，其解密后的差别也非常大。测试中，在原始秘钥中选取 $key0$ 中一个值增加 10^{-16}，即 $key0 = (0.141\,592\,6 + 10^{-16}, 0.653\,589)$ 对加密音频进行解密。解密后的音频时域波形图杂乱无章，得到完全错误的解密音频，无法识别出原始音频的信息，如图 7 所示。对于一个安全的加密算法，其密钥空间大小至少超过 2^{100} 才算是安全有效的加密算法。本文加密算法中共有 2 组 7 个秘钥，密钥空间为 $(10^{16})^7 >> 2^{372} >> 2^{100}$，密钥空间足够抵御穷举攻击。

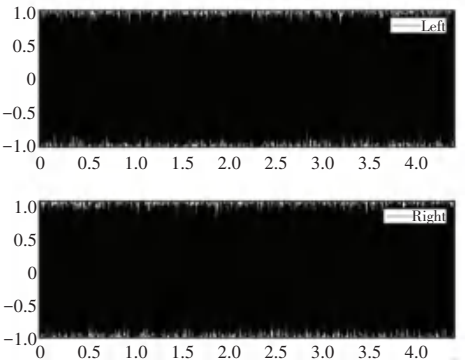


图 7　错误秘钥解密音频时域波形图

Fig. 7　Wrong key decryption audio time domain waveform

3.3　抗统计攻击性能分析

3.3.1　语谱图分析

音频的语谱图将整个音频范围用不同的颜色记录，这些颜色表示特定时间、特定频率与能量之间的关系[8]。图 8(a)、(b)分别显示了原始音频与加密音频的语谱图。表 2 为原始音频与加密音频能量分布描述统计，原始音频能量均值为 -102.488 4 dB/Hz，其标准差较大，变异度为 81.25%，分布离散，原始音频信号语谱图中能量分布不均匀，其包含较多信息量。而加密音频能量的均值为 -50.764 5 dB/Hz，标准差不大，变异度为 11.24%，表明加密音频能量均匀分布在 -50.764 5 dB/Hz 附近，几乎不包含原始音频信息，音频整体平均能量分布也被拉高，接近噪声，可以抵御基于音频语谱图的统计攻击。

3.3.2　信息熵分析

一条信息所包含信息量的大小取决于信息的不确定程度，而其不确定程度与复杂度由信息熵来量化。信息熵数学定义为：

$$H(A) = -\sum_{i=0}^{2^8-1} p(a(i))\log_2 p(a(i)) \qquad (8)$$

信息熵越大，则信息的不确定程度与复杂度越大。加密后的音频数据信息熵越接近 8，加密效果越好，音频越接近于噪声，攻击者获取的信息越少。

由表 3 可以看出，加密后的音频左右声道信息熵都接近于 8，加密音频信号混乱接近噪声，表明该加密算法能够抵御基于音频信息熵的统计攻击。

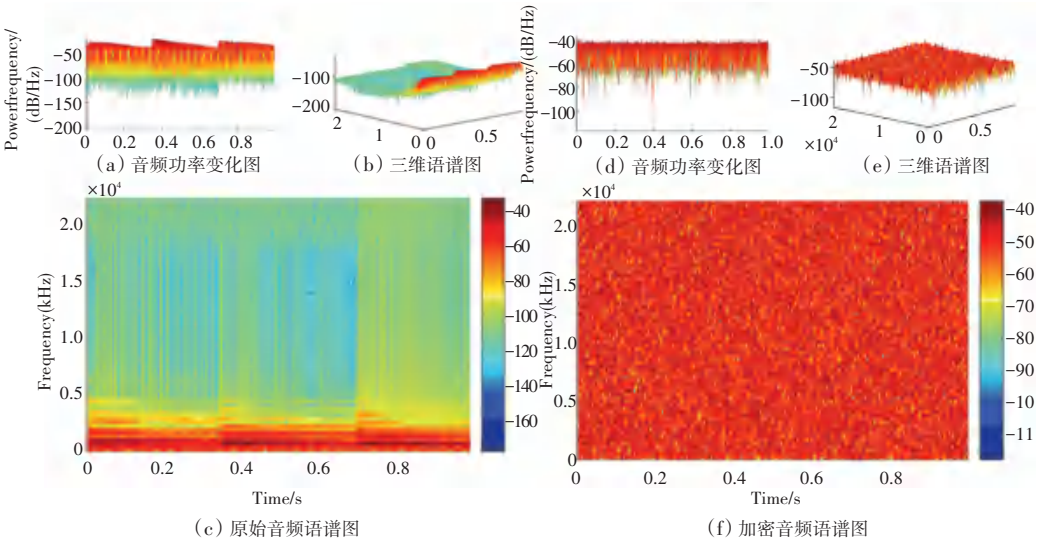


图 8 原始音频声与加密音频声谱图

Fig. 8 Original audio encrypted audio spectrogram

表 2 音频能量分布描述统计表(dB/Hz)

Tab. 2 Description of audio magnitude distribution

	mean	std	CV/%
原始音频	−102.488 4	83.270 1	−81.25
加密音频	−50.764 5	5.704 0	−11.24

表 3 信息熵对比表

Tab. 3 Comparison table of information entropy

加密方案	信息熵	
	L	R
原始音频	7.106 1	6.968 0
加密音频	7.999 3	7.999 6
文献[9]	7.998 1	7.998 7
文献[10]	7.998 8	7.998 5
文献[11]	7.499 1	7.498 9

加密音频数据整体在区间内概率分布越均匀,加密音频的抗统计攻击性能越优。直方图横轴为分布区间,纵轴为对应的频数或频率。图 9 分别为原始音频与加密音频频数分布直方图。

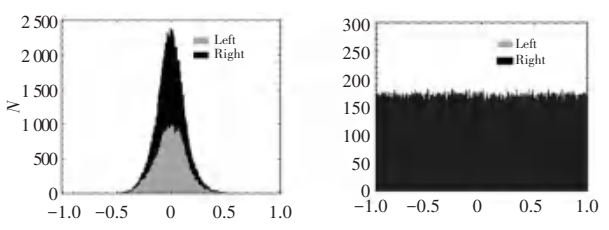


图 9 原始音频与加密音频直方图

Fig. 9 Histograms of raw and encrypted aud

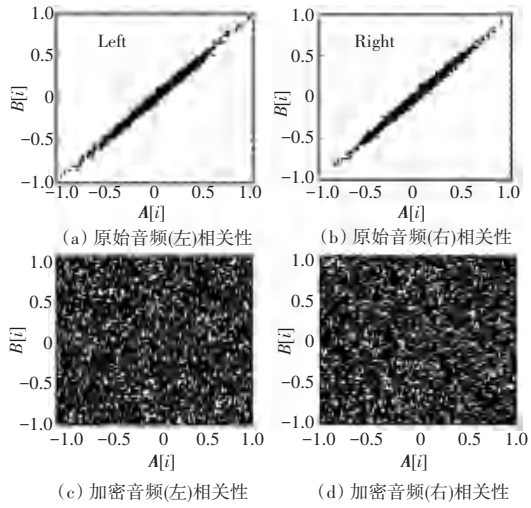
由图 9 中可以直观的看出,原始音频的频数分布近似正态分布,而加密音频的频数分布均匀,很好的隐藏了原始音频的统计特性,攻击者不易通过分析密文直方图获得信息,从而能够抵抗基于直方图的统计攻击。

3.3.3 相关性分析

加密音频相邻采样数据之间相关系数越小,说明数据的混乱与复杂程度越大,因而加密安全性更高。音频相邻幅值间相关系数计算公式如下:

$$r = \frac{\sum_{i=1}^{n} (\boldsymbol{A}[i] - \bar{\boldsymbol{A}})(\boldsymbol{B}[i] - \bar{\boldsymbol{B}})}{\sqrt{\sum_{i=1}^{n} (\boldsymbol{A}[i] - \bar{\boldsymbol{A}})^2 \sum_{i=1}^{n} (\boldsymbol{B}[i] - \bar{\boldsymbol{B}})^2}} \tag{9}$$

其中存储向量 $\boldsymbol{A}[i]$ 和 $\boldsymbol{B}[i]$ 表示第 i 对相邻音频信号值,n 为总对数。随机选取 10 000 对相邻音频数据进行测度。图 10 为明文音频与加密音频相邻幅值散点图,图中可以看出明文音频左右声道相邻音频信号值之间呈现出明显相关关系,而加密音频相邻音频信号值之间无相关关系,表 4 为相邻音频信号相关性对比表,表中明文音频左右声道相邻信号值相关性为正相关关系数值分别为 0.994 3 与 0.997 2,而加密音频左右声道相邻信号值相关系数分别为 0.000 7 与−0.000 3 接近于 0 表明其无相关关系,通过与其他文献对比文中加密算法加密后的音频混乱与复杂程度大,攻击者不易通过分析相关性操作得到明文音频信息. 表明加密算法能够很好的抵御基于相关性的统计攻击。



(a) 原始音频(左)相关性　(b) 原始音频(右)相关性

(c) 加密音频(左)相关性　(d) 加密音频(右)相关性

图 10　明文音频与加密音频相邻幅值散点图

Fig. 10　Adjacent amplitude scatter plot of plain-text audio and encrypted audio

表 4　相邻音频信号相关性对比表

Tab. 4　Correlation comparison table of adjacent audio signals

加密方案	相邻信号相关性	
	L	R
Original Audio	0.994 3	0.997 2
Ciphered Audio	0.000 7	−0.000 3
文献[12]	0.003 8	−0.005 2
文献[13]	0.061 6	0.062 7
文献[14]	−0.024 1	0.015 4

3.3.4　峰值信噪比分析 (*PSNR*)

峰值信噪比为音频信号最大功率与噪声音频信号功率的比值。峰值信噪比常用作确定信号压缩质量,数值越大,信号压缩质量越高,越接近原始音频。若加密音频与明文音频峰值信噪比越低,则加密音频与原始音频差异越大,加密后的音频越接近噪声。峰值信噪比通过均方误差(*MSE*) 来定义,均方误差反映了两组信号之间的差异程度。均方误差与峰值信噪比的计算如下:

$$MSE = \frac{1}{fs}\sum_{i=1}^{fs}\left(a(i) - c(i)\right)^2 \tag{10}$$

$$PSNR = 10\log_{10}\left(\frac{MAX(a)}{\sqrt{MSE}}\right)^2 \tag{11}$$

其中, $a(i)$ 为原始音频序列,$c(i)$ 为加密音频序列。

表 5 中列出了随机选取的 5 段加密音频 *PSNR* 测试结果。可以看出,加密后的音频在不同长度下左右声道的峰值信噪比都较低,加密音频与原始音频差别较大,加密后的音频很好的隐藏了原始音频的信息,表明该加密算法能够很好的抵御基于峰值信噪比的统计攻击。

表 5　加密音频 *PSNR* 测试结果表

Tab. 5　Test results of encrypted audio *PSNR*

	MSE (Left)	*PSNR* (Left)	*MSE* (Right)	*PSNR* (Right)
Audio1_1	0.382 5	2.391 8	0.347 1	2.708 1
Audio1_2	0.384 3	3.006 7	0.399 7	3.507 1
Audio1_3	0.353 6	1.855 9	0.349 9	1.872 8
文献[10]	/	−0.530 8	/	/
文献[11]	0.270 4	4.876 1	/	/
文献[12]	/	27.304 5	/	/

3.4　鲁棒性分析

3.4.1　抵抗差分攻击性能分析

攻击者通过对原始音频进行细微差别的改变,分析加密音频之间映射出的差异情况,这种类型的攻击称为差分攻击。

在数据加密中对差分攻击的抵抗性能一般通过样本数变化率 (*NSCR*) 和统一平均变化强度 (*UACI*) 进行分析。

NSCR 是对加密算法质量的鲁棒性检验,测试目的是原始音频和对应加密音频间不同样本数量在样本总数中所占比例的比较。计算公式如式(12):

$$NSCR = \frac{\sum_{i=1}^{fs}\left|Sign(C(i) - C'(i))\right|}{fs} \times 100\% \tag{12}$$

其中, $C(i)$ 为未改变原始音频的加密音频序列; $C'(i)$ 为随机改变一个原始音频采样数据的加密音频序列; $Sign(\,)$ 为符号函数。

UACI 是记录原始音频与加密音频相应位置差值与最大差值间比值的平均值,计算公式如式(13):

$$UACI = \frac{1}{fs}\sum_{i=1}^{fs}\frac{\left|C(i) - C'(i)\right|}{2^8 - 1} \times 100\% \tag{13}$$

当音频信号为 8 bit 时,加密算法抗差分攻击的 *NSCR* 和 *UACI* 的最优值分别为 100% 和 33.333%。

表 6 为随机测试30 000段加密音频的 *NSCR* 和 *UACI* 平均值对比。通过与其它文献对比分析表明:本文音频加密算法得到的 *NSCR* 与 *UACI* 更加接近理想值,加密算法的抵抗差分攻击性能较强。

表 6　随机测试 *NSCR* 和 *UACI* 平均值对比

Tab. 6　Comparison of average values of *NSCR* and *UACI* in random tests　%

	NSCR	*UACI*
Audio1_10K	99.993 7	33.841 1
Audio1_20K	99.994 8	34.268 7
Audio1_30K	99.996 2	33.218 4
文献[13]	99.583 4	25.585 0
文献[14]	99.601 1	36.545 1
文献[15]	99.573 6	33.364 2

3.4.2 抗噪声性能分析

当攻击者进行主动攻击时,对密文加入噪声,解密信息质量会大幅度下降。加密算法的抗噪声性能越好,在密文受到噪声攻击时,解密后还原出原始音频的信息越多。在密文传输中,当攻击者对密文进行剪切攻击时,鲁棒性较差的算法在受到攻击后,密文解密后明文的关键信息会丢失,导致信息无法成功传输。优秀的算法在受到剪切攻击,密文解密后可解析的信息应尽可能多,而能够保留明文的关键信息。图 11 为加入 5%的椒盐噪声解密后的音频时域波形图。

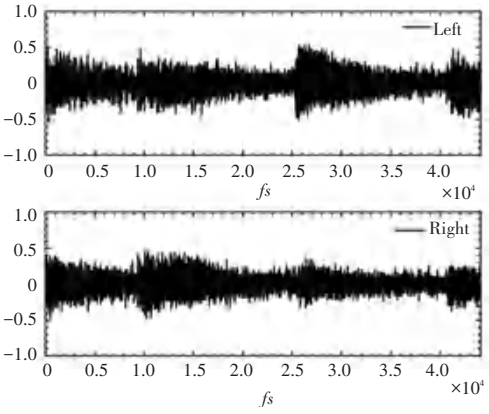


图 11 加入 5%椒盐噪声的解密音频时域波形图

Fig. 11 Decoded audio time domain waveform with 5% salt and pepper noise

由图中可以看出,在加入 5%椒盐噪声的情况下,解密后的音频时域波形质量较高,可以轻松被人耳所识别,解密后的音频依然能够恢复大部分信息。计算加入椒盐噪声后,解密音频与明文音频的峰值信噪比可以以数值形式量化音频加密算法的抗噪声性能,计算得到左右声道的均方误差分别为:7.911 0E-04、6.595 3E-04。解密音频左右声道峰值信噪比分别为:25.944 0、25.246 8。计算得到的均方误差较低,解密后音频质量较高,加密算法具有良好的抗噪声性能。

4 结束语

本文通过对二维 Hénon 混沌映射进行升维与改进得到改进的 3D-Hénon 混沌映射,并将其与离散化的超混沌 Chen 系统相结合,生成的伪随机序列用于音频加密。预处理过程将原始音频信号进行分块处理提升了运行效率,利用生成的伪随机序列进行循环排序置乱以及向前向后扩散完成加密。其中秘钥与明文音频互相关联,实现了“一次一密”,降低了选择明文攻击的可能性。通过仿真与分析结果表明,提出的音频加密算法具有较强的秘钥敏感性和足够大的秘钥空间,加密后的音频能量分布均匀,相邻振幅间相关性较低,与明文音频的峰值信噪比较低,加密算法具有良好的抗统计攻击性以及鲁棒性。

参考文献

[1] 钟艳如,刘华役,孙希延,等. 基于 2D Chebyshev-Sine 映射的图像加密算法[J]. 浙江大学学报:理学版,2019,46(2):131-141,160.

[2] GNANAJEYARAMAN R, PRASADH K, RAMAR. Audio encryption using higher dimensional chaotic map[J]. International Journal of Recent Trends in Engineering,2009,1(2),103-107.

[3] 唐素娟,张定会. 音频的混沌置乱加密[J]. 数据通信,2013(1):36-37.

[4] LIU H J, ABDURAHMAN K, LI Y L. Audio encryption scheme by confusion and diffusion based on multi-scroll chaotic system and one-time keys[J]. Optik - International Journal for Light and Electron Optics,2016,1-13.

[5] 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.

[6] 蒲越,李国东,赵静. 基于细胞神经网络混沌特性的音频加密技术应用[J]. 云南大学学报(自然科学版),2017,39(4):539-546.

[7] GAO T G, CHEN G R, CHEN Z Q, CANG S J. The generation and circuit implementation of a new hyper-chaos based upon Lorenz system[J]. Physics Letters A,2007,361(1-2):78-86.

[8] AZIZ H,GILANI S M M, HUSSAIN I, et al. A Noise-Tolerant Audio Encryption Framework Des-igned by the Application of S8 Symmetric Group and Chaotic Systems[J]. Mathematical Problems in Engineering,2021,2021:1-15.

[9] BABU N R,KALPANA M, BALASUBRAMANIAM P. A novel audio encryption approach via fin-ite-time synchronization of fractional order hyperchaotic system[J]. Multimedia Tools and Applications, 2021, 80(12): 18043-18067.

[10] ADHIKARI S, KARFORMA S. A novel audio encryption method using Henon-Tent chaotic pseudo random number sequence[J]. International Journal of Information Technology, 2021, 13(4): 1463-1471.

[11] NASKAR P K, BHATTACHARYYA S, CHAUDHURI A. An audio encryption based on distinct k-ey blocks along with PWLCM and ECA[J]. Nonlinear Dynamics,2021,103(2):2019-2042.

[12] ABDELFATAH R I. Audio encryption scheme using self-adaptive bit scrambling and two multi cha-otic-based dynamic DNA computations[J]. IEEE Access, 2020, 8: 69894-69907.

[13] SOLIMAN N F, KHALIL M I, ALGARNI A D, et al. Efficient HEVC steganography approach ba-sed on audio compression and encryption in QFFT domain for secure multimedia communication [J]. Multimedia Tools and Applications, 2021, 80(3): 4789-4823.

[14] SHAH D, SHAH T, JAMAL S S. Digital audio signals encryption by Mobius transformation and H-énon map [J] Multimedia Systems,2020,26(2):235-245.

[15] AL-KATEEB Z N, MOHAMMED S J. A novel approach for audio file encryption using hand geometry[J]. Multimedia Tools and Applications,2020,79(27): 19615-19628.