

基于动态可变参数的复合混沌系统的语音加密算法研究

龚雪¹, 张育钊¹, 庄铭杰¹, 唐加能^{1,2,3}

(1. 华侨大学工学院, 福建泉州, 362021;
2. 华侨大学机电及自动化学院, 福建厦门, 361021;
3. 福建先创电子有限公司, 福建泉州, 362000)

摘要: 利用混沌理论, 基于 Hénon 映射和 Logistic 映射设计了一个复合混沌系统, 并证明了其具有更好的初值敏感性。对产生的混沌二值序列进行美国国家标准与技术研究所(National Institute of Standard and Technology, NIST)随机数测试, 分析得出该序列具有较好的随机性, 可用于加密。依此设计了一个语音加密算法, 实现了语音信号的加/解密功能。仿真分析表明, 该混沌语音加密算法具有较高的安全性, 能产生足够的密钥空间, 有较强的保密性能。

关键词: 复合混沌系统; Logistic 映射; Hénon 映射; 语音加密

中图分类号: H107

文献标识码: A

文章编号: 1000-3630(2016)-06-0542-08

DOI 编码: 10.16300/j.cnki.1000-3630.2016.06.011

A novel voice encryption algorithm based on hybrid chaotic system with variable parameter

GONG Xue¹, ZHANG Yu-zhao¹, ZHUANG Ming-jie¹, TANG Jia-neng^{1,2,3}

(1. College of Engineering, Huaqiao University, Quanzhou 362021, Fujian, China;
2. College of mechanical engineering and automation, Huaqiao University, Xiamen 361021, Fujian, China;
3. Centron Communications Technologies Fujian Co., Ltd., Quanzhou 362021, Fujian, China)

Abstract: By use of chaos theory, a hybrid chaotic system with variable parameter is designed based on Logistic map and Hénon map in this paper, and we proved that it has higher sensitivity to initial conditions. American National Institute of Standard and Technology (NIST) statistical tests show that the chaotic sequences have good pseudo-randomness. Thus, it has adequate cryptographic properties in terms of randomness quality. Based on this system, a novel encryption algorithm is proposed, and the encryption and decryption function of voice signal is implemented. The simulation results show that the encryption algorithm has characteristics of high security and enough key space, and demonstrates significant cryptographic qualities at a good security level.

Key words: hybrid chaotic system; Logistic map; Hénon map; voice encryption

0 引言

随着语音通信的广泛应用, 当语音信息在开放和共享的信道和网络中传输时, 语音信息可能会面临安全问题, 特别是当语音信息中携带敏感信息时, 其安全会受到威胁。对于军事、公安、政府等部门来说, 语音信息的加密传输显得至关重要。

早期的语音加密算法主要是模拟加密, 随着数字通信技术的飞速发展, 一些学者开始利用数字技

术研究语音加密算法。模拟语音信号经过数字转换和压缩编码后与密钥进行加密, 得到密文。数字加密技术分为全部加密和部分加密, 全部加密是对所有的语音数据进行加密, 其安全性高; 部分加密只是对语音数据中的敏感信息进行加密, 减少了加密过程中的运算量。

模拟加密分为时域加密、频域加密、变换域加密和多维域加密等方式。模拟语音加密具有简单实用、占用带宽小、音质较高、能在许多信道上使用的优点。但是模拟加密后语音的可懂度高, 安全性较差, 主要是模拟加密方法没有改变语音信号的冗余性。与模拟语音相比, 由于数字加密使用了语音压缩编码技术, 并且语音数据一直以数字化的形式存在和传递, 所以语音数字加密与模拟加密相比有更好的安全性, 但其运算量大。数字加密中通常采

收稿日期: 2016-04-08; 修回日期: 2016-07-20

基金项目: 国家自然科学基金资助项目(61573004); 福建省教育厅项目(JA15035); 泉州市科技项目(2014Z103, 2015Z114)

作者简介: 龚雪(1992—), 女, 湖北应城人, 硕士研究生, 研究方向为计算机技术在移动通信系统中的应用。

通讯作者: 龚雪, E-mail: yuri_gx@163.com

用的是 DES(Data Encryption Standard, DES)、AES(Advanced Encryption Standard, AES)、RSA(Rivest Shamir Adleman, RSA)等传统密码学算法。

由于语音信号具有数据量大、冗余性、高度自相关和传输具有实时性的特点, DES、AES、RSA 等传统的密码学算法不再合适^[1]。为了解决语音通信中的安全问题, 一些语音加密算法相继被提出。在这些加密算法中, 混沌加密技术被视为能有效地解决语音信号数据量大、冗余度高的问题。许多学者相继提出了有效的混沌加密算法。文献[2]提出了利用混沌切换系统来加密语音信号, 先将语音数据分组, 然后利用不同混沌系统产生的混沌序列进行加密, 但是其不适用于加密大量的语音数据。文献[3]利用 Circle 映射产生的密钥序列来置乱语音信号的位置; 利用 Logistic 映射产生的密钥序列来改变语音信号的幅值。文献[4]基于 Lorenz 混沌系统簇产生了随机性好的混沌序列, 通过异或操作加密语音数据。文献[5]提出了利用分数阶 Lorenz 混沌系统设计了双通道语音加密系统, 利用拉普拉斯变换实现了发送端和接收端的混沌同步。文献[6]混合两个 Logistic 映射产生的密钥流对语音信号进行加密, 用一个 Logistic 映射的输出作为另外一个 Logistic 映射的输入, 使系统具有更好的混沌特性。

混沌系统具有初值敏感性, 产生的混沌序列具有良好的伪随机性, 其结构复杂并且难以预测和分析。利用混沌理论设计加密算法, 关键是产生随机性良好的混沌序列^[7-12]。理论上, 混沌序列周期趋于无穷, 具有接近于白噪声的相关函数。但实际应用过程中, 由于计算机和数字电路的计算精度有限, 混沌序列会出现短周期现象, 混沌系统性能会受到一定的影响。为了在有限精度下产生伪随机性好的混沌序列, 文献[13]中提出一种变参数复合混沌系统, 通过判断一个子系统迭代值小数点后某一位的状态, 使得另一个子混沌系统的分岔参数为两个固定数值中的某一个。但是, 对该系统产生的混沌序列进行美国国家标准与技术研究所(National Institute of Standard and Technology, NIST)随机数测试时, 发现其并不能通过所有的测试, 说明其并不具有好的伪随机性。与此同时, 分析得到该混沌系统的密钥只有 4 个, 因此密钥空间较小。

为此, 本文提出了一种动态变参数复合混沌系统, 其由 Hénon 映射和 Logistic 映射级联组成, 迭代过程中子混沌系统的分岔参数不断变化。一方面采用二维混沌系统使得密钥参数有所增加, 扩大了密钥空间; 另一方面混沌系统的分岔参数是动态变

化的, 减弱了有限精度效应影响, 增大了混沌序列的周期。通过随机数测试和安全性分析, 验证了该混沌序列具有较好的伪随机性和能有效地抵抗统计分析。

1 复合混沌系统设计

混沌系统具有可加性, 文献[14]从理论和仿真两个角度说明了混沌现象具有可加性, 由两个简单混沌系统构成的新系统也是一个混沌系统, 复合混沌系统的动力学行为是在单一系统的基础上演变而来的。

1.1 低维混沌映射

混沌映射是用于产生混沌序列的动力学过程。本文研究的混沌映射包括 Logistic 映射和 Hénon 映射。Logistic 映射^[15]是一种经典的一维混沌映射, 定义如下:

$$x(n+1) = \mu x(n)(1-x(n)) \quad (1)$$

其中: $\mu \in (0, 4]$ 为分岔参数, $x \in (0, 1)$ 。对于不同的 μ 值, 系统将呈现不同的特性, 随着参数 μ 的增加, 系统不断经历倍周期分岔, 当 $3.57 \leq \mu < 4$ 时, 系统进入混沌状态。

Hénon 映射^[16]是二维离散混沌映射, 其定义如下:

$$\begin{cases} y_1(n+1) = 1 - ay_1(n) + y_2(n) \\ y_2(n+1) = by_1(n) \end{cases} \quad (2)$$

当 $7 \leq a \leq 1.4$ 、 $b = 0.3$ 时, 系统进入混沌状态。 a 为分岔参数, 变量 $y_1 \in (-1.5, 1.5)$, 当 $a = 1.4$ 时, 系统复杂度最大。

1.2 复合混沌系统

基于低维混沌映射的加密算法具有运算量小、实现简单的特点, 但其密钥空间小, 因此安全性较差。为了提高混沌加密系统的复杂度和安全性, 文中采用了混沌系统级联的方式。为了减弱有限精度效应造成的混沌序列短周期现象, 对分岔参数进行扰动, 进而扩大混沌序列周期。

本文混沌加密系统由 Logistic 映射和 Hénon 映射级联组成。组成复合混沌系统的子系统通过输出状态来改变另一子混沌系统的分岔参数, 实现子混沌系统之间的相互作用和分岔参数的动态变化。复合混沌系统原理框图如图 1 所示。

采用动态调整的方式不断改变分岔参数 μ 和 a 的大小。文献[17]中, 针对单一的 Logistic 映射提出了一种动态改变分岔参数的方式, 改善了混沌序

列周期。本文在此基础上提出利用复合混沌中子系统输出状态变量来改变另一个子混沌系统中分岔参数。扰动分岔参数的数学模型如下：

$$\begin{cases} \mu_{n+1} = \mu_n + c|y_n|/2^n \\ a_{n+1} = a_n + cx_n/2^n \end{cases} \quad (3)$$

由式(3)推导可得：

$$\begin{cases} \mu_{n+1} = \mu_1 + c|y_n|/2 + c|y_n|/2^2 + \dots + c|y_n|/2^n \\ a_{n+1} = a_1 + cx_n/2 + cx_n/2^2 + \dots + cx_n/2^n \end{cases} \quad (4)$$

其中： x_n 、 y_n 为混沌系统迭代值， c 为加权系数。当分岔参数 μ 的值越接近于4、 a 的值越接近1.4时，混沌系统有更好的混沌特性^[18-19]。取加权系数 c 的值为0.1，由于 x_n 、 $|y_n|$ 取值范围分别在(0, 1)和(0, 1.5)之间，故取初值 μ_1 、 a_1 的值分别为3.85和1.3。因此 $\mu_{n+1} \in (3.85, 4)$ ， $a_{n+1} \in (1.3, 4)$ ，保证了系统有好的混沌特性。同时，由于 μ_{n+1} 为关于 x_n 的函数， a_{n+1} 为关于 y_n 的函数，故 μ_{n+1} 和 a_{n+1} 具有良好的随机性。

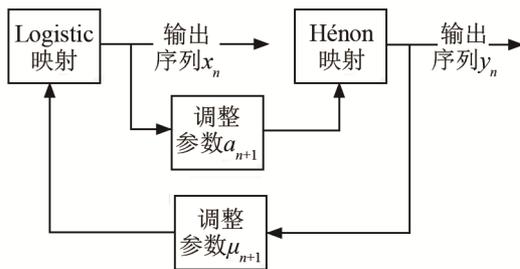


图 1 复合混沌系统原理框图
Fig.1 Block diagram of the hybrid chaotic system

1.3 混沌序列二值化

由于语音信号经过压缩编码后为二进制流，而产生的混沌序列为实数值序列，因此需要对混沌序列进行二值化处理。常用的二值化方法有符号函数二值化和比特位提取方法。由于采用符号函数方法产生的二值混沌序列具有伪随机性差的特点^[20]，为了获得随机性更好的二值混沌序列，文中采用比特位提取的方法对混沌序列进行二值化处理。

将混沌实数值序列转换为用二进制表示的形式如下：

$$x_n = 0.b_1(x_n)b_2(x_n)...b_i(x_n)...b_L(x_n) \quad (5)$$

在式(5)中， x_n 为混沌系统第 n 次迭代的结果，将其转换为用 L 位二进制浮点数表示的形式，其中 $b_i(x_n) \in (0,1)$ 是 x_n 的第 i 位。因此，混沌系统每迭代一次就可以获得 L 位比特的二值序列。在生成密钥流时，本文没有取实数值的全部二进制位，而是引进了抽取函数，即对每个实数值只抽取部分二进制位，这种方式也能增大密钥流的强度。

经过实验分析，发现当每个混沌实数值只抽取某一位二进制作为密钥时，能获得随机性较好的二值序列。

2 混沌性质研究

2.1 初值敏感性

混沌系统一个最基本的特征是对初始条件的高度敏感性，系统的Lyapunov指数可以有效地表征系统随时间演化时对初值的敏感性。因此Lyapunov指数是衡量混沌系统初值敏感度的一个重要定量指标^[21]。一维混沌映射只有一个Lyapunov指数，可以通过求混沌映射函数 $f(x)$ 在 n 时刻 x_n 处的导数来计算Lyapunov指数，其数学表达式为：

$$\lambda = \lim_{n \rightarrow \infty} \lambda_n = \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x)| \quad (6)$$

当 $\lambda < 0$ 时，表明混沌系统运动轨道是稳定的对应周期运动；当 $\lambda > 0$ 时，表明混沌系统运动轨道不稳定，对应混沌状态。

本文在对比实验中，分别取Logistic映射和Hénon映射的分岔参数为4和1.4，求得其Lyapunov指数如表1所示。由复合混沌系统的Lyapunov指数近似等于各级联子系统的Lyapunov指数之和^[22]，可以计算得本文复合混沌系统的Lyapunov指数。从表1中可以看出，复合混沌系统具有更高的Lyapunov指数，即本文复合混沌系统具有更高的初值敏感性。

表 1 Lyapunov 指数比较
Table 1 The comparison of Lyapunov exponent

	Logistic 映射	Hénon 映射	复合混沌系统
Lyapunov 指数	0.69	0.418	0.970 1

为了进一步说明混沌系统的初值敏感性，在仿真过程中，改变初值，使得误差 $\Delta = 10^{-10}$ ，对比复合混沌系统中子系统和单一混沌映射在两个不同初值下输出序列的差值。图2中横轴表示迭代次数，纵轴表示在初值 x_0 和 x'_0 、 y_0 和 y'_0 下产生的混沌序列的差值。对比图2(a)和图2(b)可以得到，经过约2步迭代后，复合混沌系统中的Logistic映射有明显的差值波动，而单一Logistic映射大约经过30步才有比较明显的差值波动；对比图2(c)和图2(d)中可以得到，Hénon映射大约迭代40步以后，才出现差值波动，而复合混沌系统中的Hénon映射经过约2步即出现差值波动。这充分说明，与单一混沌映射相比，本文复合混沌系统具有更高的初值敏感性。

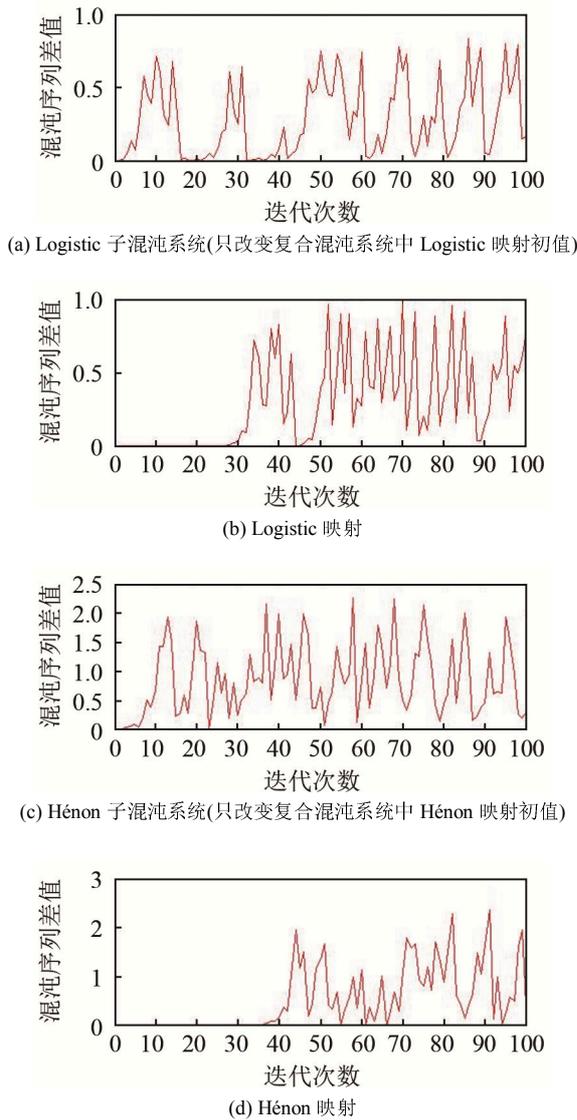


图 2 不同映射的混沌序列差值迭代图

Fig.2 Iterative graphs of chaotic sequence differences for different maps

表 2 分别列出了复合混沌系统中 Logistic 子映射和 Hénon 子映射以及文献[13]中抛物线映射和人字映射迭代的差值结果。由表 2 分析可得，本文复合混沌系统中的 Logistic 映射和 Hénon 映射在迭代

表 2 不同映射的混沌序列差值迭代结果

Table 2 Iterative results of chaotic sequence differences for different maps

n	Logistic	Hénon	抛物线映射	人字映射
1	$1.000\ 0 \times 10^{-10}$	$1.000\ 0 \times 10^{-10}$	$1.145\ 2 \times 10^{-10}$	$2.383\ 3 \times 10^{-10}$
2	0.013 3	0.010 9	$3.515\ 2 \times 10^{-9}$	$1.832\ 7 \times 10^{-8}$
3	0.048 8	0.040 4	$1.071\ 7 \times 10^{-7}$	$1.810\ 5 \times 10^{-6}$
4	0.141 8	0.055 4	$5.706\ 3 \times 10^{-6}$	$1.578\ 0 \times 10^{-4}$
5	0.076 8	0.094 4	$1.936\ 4 \times 10^{-4}$	0.013 8
6	0.264 3	0.043 2	0.014 8	0.145 5
7	0.579 3	0.261 2	0.165 9	0.081 2

2 次的时候就有了明显的差值波动，而文献[13]中的抛物线和人字映射则在迭代 6 次的时候才有明显的差值波动。因此本文复合混沌系统具有更高的初值敏感性。

2.2 相关性分析

自相关性和互相关性是混沌序列的两个重要性质。自相关性可以对序列进行周期检测；而互相关系数越小，表明序列之间的差异越大。选择自相关和互相关性较好的序列有利于提高加密算法的可靠性。

自相关和互相关函数公式为^[13]：

$$R_{xy}(k) = \lim_{N \rightarrow \infty} \frac{1}{N-k} \sum_{m=1}^{N-k} x(m)y(m+k) \quad (7)$$

由式(7)可以求出复合混沌系统中混沌序列的自相关函数和互相关函数值，如图 3 所示。从图 3 可以看出序列 $\{x_n\}$ 的自相关函数近似等于理想冲击函数，序列 $\{x_n\}$ 和 $\{y_n\}$ 的互相关函数近似等于 0。分析可得，该复合混沌系统产生的混沌序列具有较好的自相关性和互相关性。

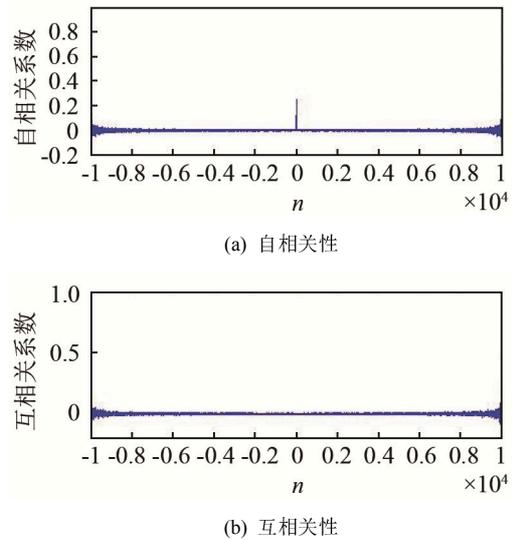


图 3 混沌序列相关性

Fig.3 Correlation functions of chaotic sequence

2.3 混沌序列随机性分析

NIST 推出的统计测试软件包 STS(Statistical Test Suite, STS)是当前测试伪随机序列系统工具中最权威的一种^[23]。本文中采用的是 2.1 版本的 STS 软件包，由 15 项核心测试组成，每项测试的结果均以 P-value 值表示。显著水平可用 α 表示，若 $P\text{-value} \geq \alpha$ ，则该项测试通过；若 $P\text{-value} < \alpha$ ，则该项测试未通过。 α 的取值范围为 $[0.0001, 0.01]$ ，通常取 $\alpha=0.01$ 。且 P-value 值越大，表明序列随机性越好。按照 NIST 测试要求，为保证测试结果的可

靠性与准确性, 每个被测序列的长度应为 $10^3 \sim 10^7$ 。实验中取被测序列长度为 10^6 比特, 分别对复合混沌系统中 Logistic 子混沌系统和 Hénon 子混沌系统以及文献[13]中抛物线映射和人字映射产生的二值序列进行随机数测试。测试结果如表 3 所示。其中*表示该项测试未通过。

表 3 NIST 随机数测试结果
Table 3 Results of NIST statistical randomness tests

测试项目	Hénon (p-value)	Logistic (p-value)	抛物线映射 (p-value)	人字映射 (p-value)
近似熵测试	0.535205	0.473786	0.990423	0.990595
块内频率测试	0.471177	0.675376	0.602877	0.061090
累积和测试 1	0.548418	0.642996	0.006376	0.271383
累积和测试 2	0.548418	0.841918	0.007275	0.532261
傅里叶变换 测试	0.274825	0.569389	0.847187	0.755036
频率测试	0.329064	0.828988	0.004568*	0.349273
线性复杂度 测试	0.815628	0.679743	0.355418	0.631790
随机偏离测试	0.903469	0.454642	0.892889	0.053175
随机偏离变量 测试	0.881949	0.605865	0.767203	0.138844
最长游程测试	0.115746	0.268352	0.498137	0.438823
重叠模块匹配 测试	0.362148	0.802678	0.250074	0.993370
非重叠模式匹 配测试	0.988997	0.941449	0.086826	0.894116
二阶矩阵阶 测试	0.619429	0.357763	0.567775	0.085113
游程测试	0.82512	0.733892	0.413378	0.424218
串行测试 1	0.778746	0.653433	0.378837	0.047676
串行测试 2	0.313304	0.879155	0.029285	0.445004
通用统计测试	0.105991	0.383026	0.483802	0.382073

对测试结果分析可知, 复合混沌系统产生的两列混沌序列全部通过测试。说明复合混沌系统产生的混沌序列具有较好的随机性, 而文献[13]中抛物线映射产生的混沌序列未能通过频率测试, 由于频率测试是用于确定序列中‘0’和‘1’个数是否相等, 因此其产生的混沌序列并不具有较好的随机性。

经过多次仿真得到, Logistic 映射取二值序列的第 11、13、14、16 位, Hénon 映射取第 10、12、13、14、15 位时, 产生的密钥流序列能通过 NIST 随机数测试。抛物线映射只有在抽取第 15 位时, 能获得随机性相对于其他位较好的密钥流序列, 但仍然有一项测试未通过; 人字映射在抽取第 10、12、16 位时能通过 NIST 随机数测试。分析可得, 与文献[13]中复合混沌系统相比, 相同计算精度下本文的复合混沌系统能产生更多的随机序列, 且其随机

性更好。

3 语音加密算法设计

3.1 语音文件预处理

本文在 Matlab 仿真环境下, 采用了 TIMIT 语音库。TIMIT 语音库为常用语音库, 适用于语音识别、说话人识别等语音信号处理研究。文中选取了 12 段语音, 分别为 6 段男声和 6 段女声, 这些语音都是一些英语长句。语音信号经过 ADPCM (Adaptive Differential Pulse Code Modulation, ADPCM) 语音压缩编码后得到语音明文二值序列 $\{M_i\}$ 。下文中, 只列出了某一语音样本的加解密效果图。

3.2 加密算法

利用动态变参数复合混沌系统迭代产生混沌序列, 然后将其转化为二值序列, 作为密钥与明文序列逐位异或操作。文中复合混沌系统产生了两列互不相关的密钥序列 $\{x_i\}$ 、 $\{y_i\}$, 为了增强加密强度, 加密过程中语音明文与两列密钥序列异或运算后得到密文 C_i 。加密方程式如下:

$$C_i = M_i \oplus x_i \oplus y_i \quad (8)$$

3.3 语音加解密步骤

本文中混沌语音加密算法步骤如下:

(1) 加密密钥设置: 取初值对 $(\mu, x(0))$, $(a_1, b, y_1(0), y_2(0))$, 以及加权系数 c 分别赋值给 Logistic 子混沌系统和 Hénon 子混沌系统;

(2) Matlab 读入一段原始语音, 利用 ADPCM 算法对语音压缩编码后得到 L 比特明文序列 $\{M_i\}$;

(3) 利用复合混沌系统迭代产生长度为 L 比特的两列密钥流序列 $\{x_i\}$ 、 $\{y_i\}$;

(4) 利用密钥流序列 $\{x_i\}$ 与语音明文序列进行异或操作, 得到密文 $P_i = x_i \oplus M_i$;

(5) 利用密钥流序列 $\{y_i\}$ 与密文 P_i 进行异或操作, 得到密文 $C_i = P_i \oplus y_i$, 即当前语音数据加密后的密文。

解密过程为加密过程的逆过程, 即明文 $M_i = C_i \oplus y_i \oplus x_i$ 。

4 算法性能分析与仿真结果

文献[12]中提出了一种利用 Chen 系统和 Lorenz 系统产生混合密钥流的语音加密算法, 其效果图如图 4 所示。比较加/解密前后语音信号时域

图可以得到，加密后语音信号波形图杂乱无章，高度不规则，解密的语音波形图类似于原始语音信号波形图，该加密算法有较好的加密效果。

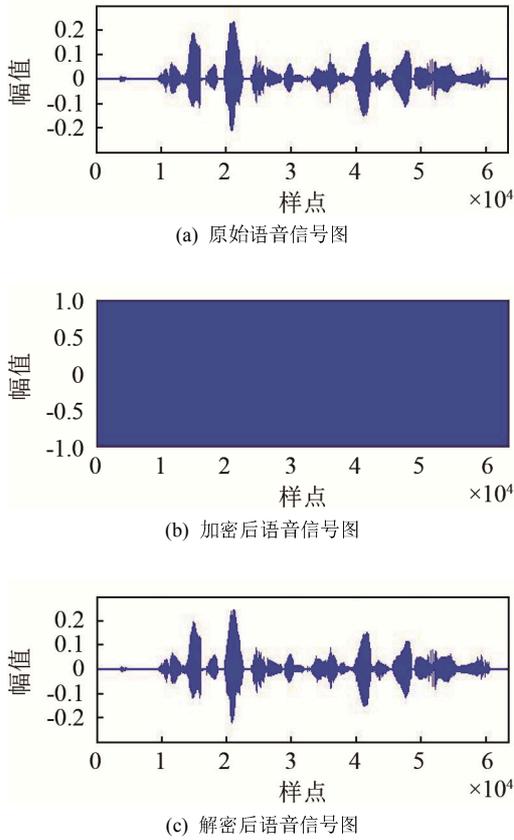


图 4 语音信号加密图

4.1 波形图与功率谱密度分析

本文实验中选择与上述相同的语音样本，即用 TIMIT 语音库作为原始语音，通过 Matlab 仿真实现语音数据加/解密。

图 5(a)为原始语音信号的波形图，图 5(b)为加密后的语音信号波形图，图 5(c)为解密后的语音信号波形图。由图 5(b)可以得到，加密后的语音信号波形图杂乱无章、高度不规则，在 Matlab 中利用 sound 命令播放加密后语音，听者只能听到刺耳的噪声且听不到任何有用信息；由图 5(c)可以得到，解密后的语音信号波形图与原始语音信号的波形图非常相近，有相同的频率分量，听者可以清楚地听到解密后的语音信息。

功率谱密度表示平均功率在频域的分布，白噪声的功率谱密度在整个频域内均匀分布。由图 6(a)和 6(b)可以看出，经过加密后的语音功率谱密度图更为平坦，在整个频域内分布较为均匀，类似于白噪声频谱。

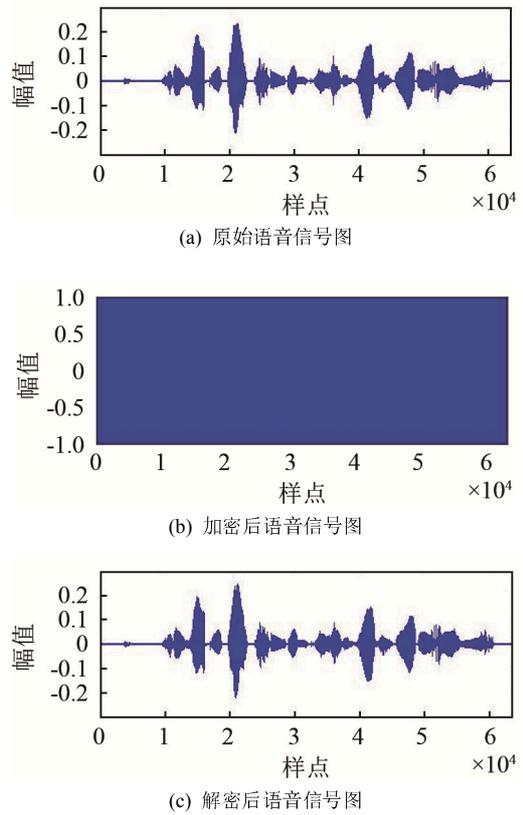


图 5 语音信号加密图
Fig.5 Encryption of voice signal

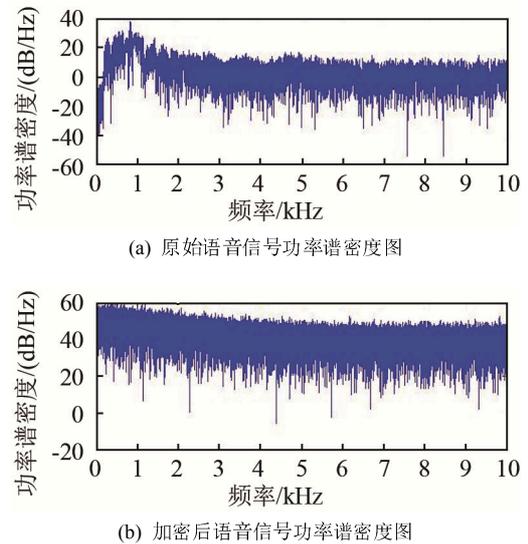


图 6 加密前后的语音信号功率谱图
Fig.6 The power spectral densities of the original and encrypted voice signals

4.2 主观评价加解密效果

为了判断加密后的语言信息是否听得懂以及解密后的语音信息是否正确，主观听辨评价^[9,24,25]中分别找来了 5 名男性和 5 名女性，对加密后密文是否能听懂以及能否听出说话人、解密后的语音能否听清楚作出评判。本文试验中 10 名测听者对

12 个语音样本加/解密后的语音效果进行打分, 平均各人的打分结果, 得到加密和解密后语音效果平均主观意见分 MOS(Mean Opinion Score, MOS)。MOS 就是对语音信号加/解密效果的最终评价分, 测得结果如表 4 所示。在数字语音通信中, 通常认为 MOS 分为 3.5 左右时能维持正常语音通信, 这时能感到语音质量有所下降, 但不妨碍正常通话, 可以满足多数语音通信系统使用要求; 当 MOS 分为 1 左右时, 说明语音效果极差, 人耳听不清或者是语音含有较大杂音。由表 4 可以看出, 加密后的 MOS 分接近为 1, 说明加密操作后, 语音信息类似于噪音, 人耳听不清有用语音信息。而解密操作后, MOS 分较高, 人耳可以听清语音信息。

表 4 MOS 值
Table 4 Value of MOS

语音样本编号	加密后 MOS 值	解密后 MOS 值
1	1	3.6
2	1.3	3.7
3	1.1	3.4
4	1	3.5
5	1	3.6
6	1.2	3.5
7	1	3.6
8	1.1	3.5
9	1.1	3.6
10	1	3.4
11	1.1	3.7
12	1	3.5

4.3 三种算法性能分析

本文实验中, 分别用本文加密算法、文献[12]中加密算法, 及对文献[13]中复合混沌系统产生的混沌序列二值化后对同一段语音加/解密, 语音信息大小为 253 952 字节。加密时间如表 5 所示。

文献[12]中采用了 Lorenz 和 Chen 两种高维混沌系统, 因此系统具有较高的复杂度。但在仿真过程中, 语音加密所需时间大约为本文算法的 3 倍多; 利用文献[13]中混沌序列加密所需时间与本文基本相等, 但通过 2.3 节混沌序列随机性分析可以得出, 本文能产生更多随机性好的混沌序列。

表 5 加密时间比较
Table 5 Comparison of encrypt time

算法	加密时间/s
文献[12]加密算法	365.428 196
本文算法	100.643 128
文献[13]加密算法	102.235 116

综上所述, 本文构造的复合混沌系统, 在不增加计算量的前提下提高了系统的复杂度和增大了混沌序列周期, 可以满足安全性要求。

4.4 密钥敏感性分析

为了验证本算法对密钥的敏感程度, 微小改变复合混沌系统中某一混沌子映射的参数, 使得误差 $\Delta=10^{-16}$, 其他参数和初值保持不变。得到解密后的语音信号波形图如图 7 所示。可以看出, 解密后的语音波形图与原始语音信号的波形图完全不一样, 解密失败。测试表明, 文中混沌加密算法对初值十分敏感, 密钥有任何微小的改变, 都会导致解密失败, 这种初值敏感性也保证了算法的安全性。



图 7 密钥敏感性测试结果
Fig.7 The sensitivity test result of encryption keys

4.5 安全性分析

由于本文加密算法为序列加密, 首先考虑序列的安全性。序列的安全性主要由序列本身的复杂度和产生方式决定。NIST 测试中, 近似熵测试能在一定程度上反映混沌序列的复杂度, 在上文分析中, 复合混沌系统产生的二值混沌序列均通过了近似熵测试, 说明该混沌序列具有较高的复杂度。对于复合混沌系统而言, 由于其分岔参数在不断变化中, 且其具有很好的初值敏感性, 即初值任何微小的变化都会对序列的产生造成极大的影响, 因此很难通过分析得到复合混沌系统原型。

密钥空间是加密算法中所有密钥的总数, 本文算法中包括了初值 $x(0)$ 、 $y_1(0)$ 、 $y_2(0)$ 、分岔参数 μ_1 、 a_1 、 b 和加权系数 c 共七个参数, 其精度为 10^{-16} , 因此其密钥空间为 $10^{112} \approx 2^{373}$, 可以有效抵抗暴力攻击。综上所述, 本文所涉及的加密算法具有很高的安全性, 可以用于语音加密中。

5 结 论

本文基于混沌理论, 设计了一个动态变参数复合混沌系统, 产生了两列伪随机性好的二值序列。利用混沌二值序列, 对压缩编码后的语音数据进行了两次异或运算得到密文, 提高了破解难度。NIST 随机数测试表明, 复合混沌系统产生的二值混沌序

列具有较好的随机性。算法分析和仿真结果表明, 该语音加密算法实现简单, 加密效果好, 密钥敏感性强。

参 考 文 献

- [1] Hermassi H, Hamdi M, Rhouma R, et al. A joint encryption-compression codec for speech signals using the ITU-T G.711 standard and chaotic map[J]. *Multimedia Tools and Applications*, 2015, **74**: 1-24.
- [2] Zhang Y P, Duan F, Liu X. The research of applying chaos theory to speech communicating encryption system[J]. *Advances in Multimedia, Software Engineering and Computing*, 2012, **2**(7): 197-202.
- [3] Alwahbani S M H, Bashier E B M. Speech scrambling based on chaotic maps and one time pad[M]. *Proceedings of International Conference on Computing, Electrical and Electronics Engineering*, 2013: 128-133.
- [4] Sattar B Sadkhan, Rana Saad Mohammed. Proposed random unified chaotic map as PRBG for voice encryption in wireless communication[J]. *International Conference on Communication, Management and Information Technology (ICCMIT)*, 2015, **65**(1): 314-323.
- [5] Sheu L J. A speech encryption using fractional chaotic systems[J]. *Nonlinear Dynamics*, 2011, **65**(1-2): 103-108.
- [6] Hamdi M, Rhouma R, Belghith S. An appropriate system for securing real-time voice communication based on ADPCM coding and chaotic maps[J]. *Multimedia Tools and Applications*, 2016, **56**(10): 1-24.
- [7] Deng A D, Tang J N, Zhao L, et al. The variable-interval arithmetic coding using asymptotic deterministic randomness for data compression and encryption[J]. *Journal of Statistical Computation and Simulation*, 2012, **82**(10): 1545-1555.
- [8] Li S J, Mou X Q, Cai Y, et al. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision[J]. *Computer Physics Communications*, 2003, **153**(1): 52-58.
- [9] Sadkhan S B, Mohammed R S. Proposed Random Unified Chaotic Map as PRBG for Voice Encryption in Wireless Communication[J]. *Procedia Computer Science*, 2015, **65**: 314-323.
- [10] François M, Grosge T, Barchiesi D, et al. Pseudo-random number generator based on mixing of three chaotic maps[J]. *Communications in Nonlinear Science and Numerical Simulation*, 2014, **19**(4): 887-895.
- [11] Hu H P, LIU L F, Ding N D. Pseudorandom sequence generator based on the Chen chaotic system[J]. *Computer Physics Communications*, 2013, **184**(3): 765-768.
- [12] Musheer Ahmad, Bashir Alam, Omar Farooq. Chaos Based Mixed Keystream Generation for Voice Data Encryption[J]. *International Journal on Cryptography and Information Security*, 2012, **2**(1): 36-45.
- [13] 张巍, 胡汉平, 李德华. 一种新的混沌序列生成方式[J]. *华中科技大学学报(自然科学版)*, 2001, **29**(11): 64-66.
- [14] 甘建超, 肖先赐. 混沌的可加性[J]. *物理学报*, 2003, **52**(5): 1085-1090.
- [15] Mitchell J Feigenbaum. Quantitative universality for a class of nonlinear transformations[J]. *Journal of Statistical Physics*, 1978, **19**(1): 25-52.
- [16] Grassberger P, Procaccia I. Characterization of strange attractors[J]. *Physical Review Letters*, 1983, **50**(5): 346.
- [17] 杨凌, 刘玉山, 章国升, 等. 一种改进的适用于 Ad hoc 网络的混沌加密算法[EB/OL]. 北京: 中国科技论文在线 [2009-11-09]. <http://www.paper.edu.cn/releasepaper/content/200911-214>.
- [18] YANG Ling, LIU Yushan, ZHANG Guosheng, et al. An improved chaotic encryption algorithm adaptation on the Ad hoc net[EB/OL]. Beijing: Chinese Sciencepaper Online [2009-11-09]. <http://www.paper.edu.cn/releasepaper/content/200911-214>.
- [19] François M, Defour D, Negre C. A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic[J]. *Informatica*, 2014, **38**(2): 115-124.
- [20] Tang J N, Zou C R, Wang S P, et al. Chaos synchronization of chen systems with time-varying delays[J]. *International Journal of Bifurcation & Chaos*, 2012, **22**(8): 2543-2544.
- [21] Li P, Li Z, Halang W A, et al. A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map[J]. *Physics Letters A*, 2006, **349**(6): 467-473.
- [22] Takens F. Dynamical systems and turbulence[J]. *Lecture Notes in Mathematics*, 1981, **898**(9): 366.
- [23] 王光义, 袁方. 级联混沌及其动力学特性研究[J]. *物理学报*, 2013, **62**(2): 111-120.
- [24] WANG Guangyi, YUAN Fang. Cascade Chaos and Its Dynamic Characteristics[J]. *Acta Phys. Sin*, 2013, **62**(2): 111-120.
- [25] National Institute of Standard and Technology. A statistical test suite for random and pseudorandom number generators for cryptographic applications[S/OL]. <http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf>. 2001.
- [26] 黄程韦, 金赞, 王青云, 等. 基于特征空间分解与融合的语音情感识别[J]. *信号处理*, 2010, **26**(6): 835-842.
- [27] HUANG Chengwei, JIN Yun, WANG Qingyun, et al. Speech Emotion Recognition Based on Decomposition of Feature Space and Information Fusion[J]. *Signal Processing*, 2010, **26**(6): 835-842.
- [28] 黄程韦, 金赞, 王青云, 等. 基于语音信号与心电信号的多模态情感识别[J]. *东南大学学报(自然科学版)*, 2010, **40**(5): 895-900.
- [29] HUANG Chengwei, JIN Yun, WANG Qingyun, et al. Multimodal emotion recognition based on speech and ECG signals[J]. *Journal of Southeast University(Natural Science Edition)*, 2010, **40**(5): 895-900.