基于 DSP 的混沌语音加密

丁 然,王佳伟,马青玉

(南京师范大学物理科学与技术学院,江苏 南京 210023)

[**摘要**] 基于语音加密的特殊性,利用可逆二维 Arnold 变换和改进的 Logistic 映射进行了混沌加密算法研究,并以 TMS320VC5509A 为中央处理器提出了语音加密的系统方案,实现了语音的加密和解密. 首先介绍了数据加密技术基本原理和方法,然后详细给出了混沌加密系统的软硬件设计方案,并通过 DSP 芯片实现了混沌语音加密和解密. 最后对语音信号进行了模拟仿真和测试,加解密前后的信号和频谱取得了较好的一致性,证实了该混沌语音加密算法的可行性.

[**关键词**] 混沌语音加密,Arnold 变换,Logistic 映射,DSP

[**中图分类号**]TP309.7 [**文献标志码**]A [**文章编号**]1001-4616(2014)04-0059-07

DSP Based Chaotic Voice Encryption

Ding Ran, Wang Jiawei, Ma Qingyu

(School of Physics and Technology, Nanjing Normal University, Nanjing 210023, China)

Abstract: Combining with the technologies of invertible two-dimensional Arnold transform and improved algorithm Logistic mapping, a chaotic voice encryption algorithm is investigated based on the particularity of the encryption of voice, and then a voice encryption system solution is proposed to realize the voice encryption and decryption using the Digital Signal Processor TMS320VC5509A. The basic principle and method of data encryption is first introduced and a detailed design plan of software and hardware for the chaotic voice encryption system is presented, at the same time we realize the chaotic voice encryption and decryption using the DSP chip. Finally, through simulation and experimental test for voices, the waveforms and spectrums collected before encryption and after decryption show good agreements with each other, suggesting the feasibility of the proposed chaotic voice encryption algorithm.

Key words: chaotic voice encryption, Arnold transform, Logistic mapping, DSP

伴随着语音信号形式由模拟到数字的转化,语音的加密方法从根本上发生了改变. 传统的模拟加密技术要把模拟语音信号先数字化,再利用加密算法对数字语音进行加密处理,最后再把加密处理后的数字语音转化为模拟语音,但模拟语音加密后的语音数据存在冗余性高和安全性差等缺点. 而数字语音加密技术可直接对数字化后语音数据进行压缩编码和数字语音信号传输,并且在数字化和编码过程中都可以进行加密处理. 与模拟加密相比,数字加密中的语音数据采用了语音压缩编码技术,经过压缩编码后的数据以数字信号的形式进行传输,可以实现数字跳频的通信技术[1],本文就是基于数字语音加密压缩编码技术利用混沌语音加密实现语音加密[2-8].

数字加密采用压缩编码技术,为了提高加密速度和降低运算强度,对媒体数据的加密方法主要分为完全加密和部分加密两大类. 完全加密算法[9]是对编码后的所有音频信号(普通的二进制数据)进行的加密,该种加密算法具有数据量比较大以及安全性较高的特性. 部分加密算法是对编码后的数据进行选择性的加密,其中加密内容是根据人们对语音数据那些感知程度比较强的数据进行加密而其余的部分不处理. 部分加密[10]一般采用传统的 DES、IDEA 等方法,降低了运算强度,但是加密数据也减少了.

近年来 Cat 映射和 Logistic 映射相结合的分组加密算法[11]常常用来实现语音加密. 但是目前研究者

收稿日期:2014-04-03.

基金项目:国家自然科学基金(11274176).

通讯联系人:马青玉,博士,教授,研究方向:电子技术、声学和生物医学物理. E-mail:maqingyu@njnu.edu.cn

们对该方法的研究大部分局限于计算机仿真,没有实现硬件的处理和实时应用. 本文以如何保证语音通信中通信内容的安全性为研究重点,利用 Arnold 变换和 Logistic 映射的混沌加密算法,结合 DSP 技术实现语音的加密和解密,提出了一种语音通信系统中的语音加密设计方案,采用音频编解码芯片 TLV320AIC23 完成语音信号的输入输出和实现 A/D 以及 D/A 的转换,用 TMS320VC5509A 完成对语音信号的加密和解密处理. 实验中,对单频正弦信号和多频 Rap 音乐信号进行了测试,并通过比较加密前和解密后的信号,证实了该混沌语音算法的可行性. 计算机仿真和实验测试结果证明该算法增大了密钥空间,提高了加密速度,使得语音通信具有较高的安全性.

1　混沌语音加密算法

混沌加密算法是一个能将明文数据的位置充分置乱以改变其统计特性,同时对初始条件还具有敏感性的加密算法[12]. 因此利用混沌系统对初始值和参数的敏感依赖性、拓扑传递性以及生成的混沌序列具有的非周期性和伪随机性等特点来设计混沌分组密码. 本研究采用混沌系统所具有的拓扑传递特性来对语音数据进行置乱和扩散,将可逆的二维 Arnold 变换和 Logistic 映射相结合,构造一种分组密码算法实现语音信号的加密. 该算法利用 Arnold 映射置乱语音数据块中各元素的位置,但是置乱只是在空域上的变换,还不能更好地保证语音加密的安全性,为了在加密过程中使语音数据值发生改变以及语音数据的统计特性得到充分的改变,我们利用改进的 Logistic 映射构造了替换表,在每次扩散操作时都引入一次替换操作,提高了语音加密的安全性和加密速度. 最终的算法性能分析结果表明,该分组加密算法应用于语音信号的加密处理具有很高的加密速度和安全强度[13].

1.1　Arnold 变换

Arnold 变换是一种离散的混沌映射,其映射的矩阵表示形式为:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 = \boldsymbol{D} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1, \tag{1}$$

其中 $\boldsymbol{D} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ 为变换矩阵,mod1 表示小数部分,该矩阵的特征值计算表达式为:

$$\begin{vmatrix} 1-\lambda & 1 \\ 1 & 2-\lambda \end{vmatrix} = \lambda^2 - 3\times\lambda + 1 = 0, \tag{2}$$

其中 λ 表示变换矩阵的特征值. 可以得到 Arnold 变换的两个特征值分别为 $\lambda_1 = \frac{1}{2}\times(3+\sqrt{5}) > 1$ 和 $\lambda_2 = \frac{1}{2}\times(3-\sqrt{5}) < 1$,对应的两个 Lyapunov 指数分别为 $\alpha_1 = \ln\lambda_1 > 0$ 和 $\alpha_2 = \ln\lambda_2 < 0$,可见 Arnold 变换是一种混沌映射[14]. 由于 $|\boldsymbol{D}| = 1$,该映射是一个面积始终为 1 的稳定映射,通过拉伸(通过变换矩阵的作用使 x, y 又折回原来单位矩形内)可以产生混沌运动[15].

1.2　Logistic 映射

Logistic 映射定义为:

$$x_{n+1} = y\times x_n \times (1-x_n), \tag{3}$$

式中 y 为控制变量,$y \in (0, 1.4]$,$x_n \in [0,1]$,由 y 和初始值 x_0 来控制该映射系统所产生的序列. 对于不同的 y 值,Logistic 映射系统将呈现不同的特性. 图 1 显示了 x 不同取值时 Logistic 映射迭代 1 000 次结果,(横坐标和纵坐标分别表示 y 和 x 取值范围).

从图 1 中可以看出,当 $y >= 1.075$ 时,系统进入混沌状态. 当且仅当 $y = 1.4$ 时该映射系统所产生的序列才具有典型的混沌特性. 迭代结果中存在空白窗(如图所标)和稳定窗(图中右侧黑色部分),所产生序列在(0,1)范围内不具备均匀分布等等安全问题[16,17]. 另外针对映射系统中存在的各种安全方面的问题,给出了一种改进的 Logistic 映射,其动力学系统方程为:

$$x_{n+1} = y\times k\times x_n \times (1-x_n) \bmod 1, \tag{4}$$

式中 $y \in (0,4]$,$x_n \in [0,1]$. 由 y,k 和初始值 x_0 来控制该映射系统所产生的序列. 与公式(3)相比,改进后的 Logistic 映射密钥空间增大了,而计算复杂度没变. 当 k 取 678.8 时,y 取不同值情况下,改进后的 Logistic 映射迭代的 1 000 次的结果如图 2 所示,可见不论 y 取何值,映射迭代所产生的序列都进入了混沌

状态,并且具有典型的混沌特性[18],同时迭代结果中不存在空白窗、稳定窗以及(0,1)范围分布不均匀等安全问题.

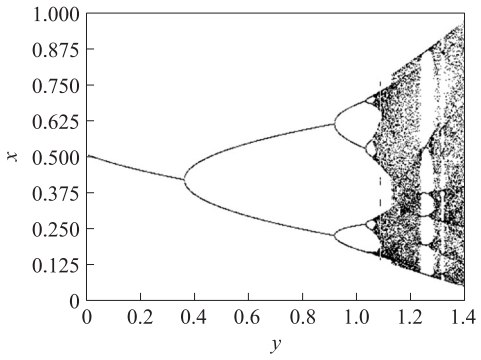

图 1　Logistic 的映射迭代结果

Fig. 1　Iteration result of Logistic mapping

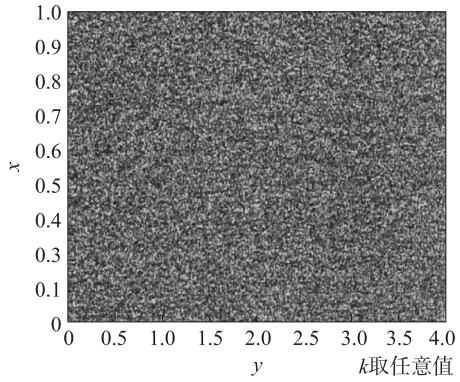

图 2　改进的 Logistic 映射迭代结果

Fig. 2　Iteration result of improved Logistic mapping

1.3　基于 Arnold 变换和 Logistic 映射的混沌加密改进算法

为了更好地实现语音的加密,保证语音信息传递的安全性,本研究的混沌加密算法采用 Arnold 变换的数据置乱和 Logistic 映射相互配合的混合加密方式. 为了将 Arnold 变换应用于加密算法中,首先应将 Arnold 变换扩展为 $N*N$,并将其离散化,相应的表达式为:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N = \boldsymbol{F} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N, \tag{5}$$

其中 $\boldsymbol{F} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix}$ 为变换矩阵,a 和 b 都为小于 N 的整数,x_n 和 y_n 表示数据在 $N*N$ 维方阵中原始位置,x_{n+1} 和 y_{n+1} 表示经过变换后数据在 $N*N$ 维方阵中的新位置. 在对方阵中的数据位置进行置乱时,是先固定好行数,然后对该行中的所有元素进行位置置乱,直至遍历到整个方阵中所有数据的位置为止.

使用改进的 Logistic 映射来构造所需的替换表,再利用产生的替换表对 Arnold 变换置乱后的明文数据按采样点进行替换操作,其替换表的构造步骤如下:

(1)将区间[0,1]均匀分成 256 个子区间$\{S_0, S_1, \cdots, S_{255}\}$,把 0 到 255 之间的整数值分别赋予给每一个区间,即 $V(S_i)=i$,记 S_i 的上界和下界分别为 $S_r(i)$ 和 $S_e(i)$,任意 S_r 中的数据 S 值都满足 $S_r(i) \leqslant S < S_e(i)$;

(2)任取 k 和初始值 x_0,进行迭代运算. 经过 P 轮迭代之后再根据迭代得到的结果所在区间记录对应的整数值. 如果第 $p(p>P)$ 次迭代获得的数值在区间 S_r 中,则得到的整数值为 t(如果迭代的结果落入已经走过的区间,不记录区间对应的整数值,使该整数值加 1,当相加后的结果大于 255 时,让该整数值对 256 取余运算,直到得到的结果取到新的整数为止,记录当前整数值),如此迭代下去,可获得一个有 256 个不重复数据的序列$\{t_0, t_1, \cdots, t_{255}\}$,其中 t_i 属于$\{0,1,2,\cdots,255\}$.

(3)原来区间[0,1]分割后对应的整数序列为$\{0,1,\cdots,255\}$,加密后的序列为$\{t_0, t_1, \cdots, t_{255}\}$,则得到新的映射关系为:$t_i = f(i)$,这就是所要构造的替换表,记为 $j=f(k)$. 由于替换表的使用使得加密速度得到提高,整个混沌语音加密的安全性也很高.

2　实验系统设计

2.1　DSP 系统的硬件设计

为了验证基于 Arnold 变换和 Logistic 映射的混沌加密改进算法在语音加密和解密应用中的可行性,我们利用 DSP 开发板进行了语音加解密的系统设计,实现对语音信号的采集、波形的存储、信号的加密和解密,语音信号的回放等功能. 系统要求能够对语音信号实现 8 kHz 的采样和还原,录音时间不低于 5 s,能够实现语音的录制、播放和加解密运算,还原的语音不存在明显失真. 针对系统的 5 个关键功能(语音采样、数据存储、加密运算、解密运算、语音还原),设计了音频数据采样模块、还原模块、批量数据计算模块、数据存储模块和系统辅助模块等功能模块.

本系统要对语音信号进行混沌加密运算,数据的运算量较大,因此采用高效的数字信号处理器(DSP)芯片来完成[19]. TMS320VC5509A 采用1.6 V 的内核电压以及3.3 V 的外围接口电压,以0.05 mW/MIP 的低功耗运行,并可以实现高达 4 MB 的外部存储空间扩展,是一款具有较高性价比的低功耗 DSP 芯片. 该芯片完全满足本次设计的需求. 针对语音的采集和处理问题,采用 TLV320AIC23 高性能立体声音频编解码芯片,对输入和输出信号具有可编程增益调节功能. TLV320AIC23 内部集成了模数转换(ADC)和数模转换(DAC)部件,采用了先进的 Σ-Δ 过采样技术,在 8 kHz 到96 kHz 的范围内提供16、20、24 和32 bit 的采样,ADC 和 DAC 的输出信噪比分别可以达到90 dB. TLV320AIC23 还具有很低的能耗,回放模式下功率仅为 23 mW,省电模式下小于 15 μW. 因此,TLV320AIC23 是一款非常理想的语音信号处理器件.

系统硬件框图如图 3 所示. 整个系统以 VC5509A 作为核心,完成语音信号的加密解密算法并且控制整个系统的运行. 音频编解码芯片 TLV320AIC23 主要用来完成语音数据的采集和回放. 模拟语音信号经过麦克风输入,通过内部的 AD 转换采集和量化输入的语音信号使之转换为 PCM 编码. PCM 编码通过 McBSP 接口发送给 DSP. DSP 对读到的 PCM 编码进行加解密处理,处理过的数据再通过 McBSP 接口发送,TLV320AIC23 读取处理后的数字语音数据,并由内部的 DA 转换为模拟语音数据通过耳机输出. VC5509A 语音信号处理时读取 GPIO3、GPIO4、GPIO6 和 GPIO7 这4 个引脚状态,来决定语音信号录音、加密、解密、播放4 种方式,并通过 CPLD 控制数码管显示工作状态.

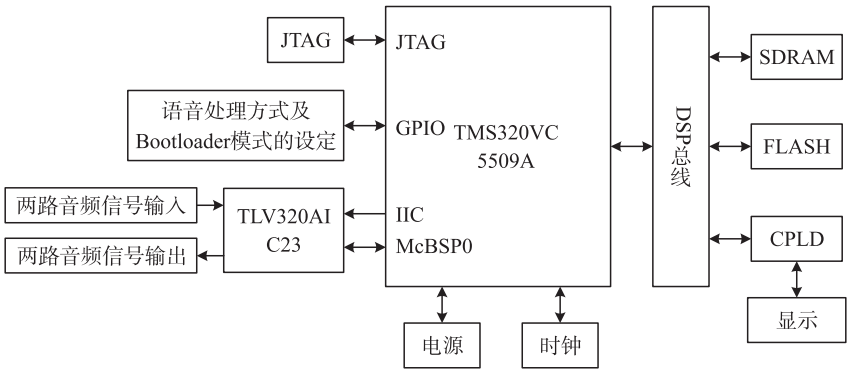

图 3　系统硬件框图

Fig. 3　Block diagram of the system

2.2　DSP 系统的软件设计

系统首先利用 DSP 对一段音频信号进行5 s 的录音,然后将录音数据通过 TLV320AIC23 音频芯片进行编解码并以 8 kHz 的频率进行数据采样,将模拟信号进行数字化处理,产生 65536 个波形数据点,并将原始语音数据存储在 SDRAM 的 0x40000-0x4FFFF 数据段;然后利用 Arnold 映射置乱对数据进行置乱加密,接着利用 Logistic 映射对数据进行混沌加密,将加密后的数据存储在 SDRAM 的 0x50000-0x5FFFF 数据段;最后通过逆向运算对加密后的数据进行解密,并将恢复的数据存储到 SDRAM 的 0x60000-0x6FFFF 数据段. 加密过程的详细步骤如下:

(1)加密密钥设置:Arnold 映射的参数 a,b 和循环轮数 l;改进后的 Logistic 映射的放大因子 k,初始值 x,迭代轮数 L,扩散操作的初始值 $C_0=K$;

(2)由改进的 Logistic 映射产生替换表;

(3)将长度为 M 的一维语音数据块按行划分为 $N*N$ 的二维方阵且满足 $M=N*N$,得到了能进行 Arnold 变换的矩阵形式;

(4)对步骤(3)得到的二维数据方阵,利用离散化后的 Arnold 映射公式进行位置置乱;

(5)每轮置乱操作之后都要进行1 次替换和扩散变换;

(6)转到步骤(4),重复步骤(4)和(5),循环做 l 轮;

(7)将置乱,替换,扩散后得到的数据块即加密后的密文,堆叠成一维向量输出.

解密与加密是互逆过程. 解密过程其步骤如下:

(1)解密密钥设置:Arnold 映射的参数 a,b 和置乱循环次数 l;改进的 Logistic 映射的放大因子 k 和初

始值 x,扩散操作的初始值 $C_0=K$,与加密密钥值相同;

(2)构造解密时所需的替换表,在加密时我们产生了替换表,这时的替换表是加密时替换表的逆过程,即 $k=f^{-1}(j)$;

(3)将加密过程产生的长度为 M 的一维密文数据块化为 $N*N$ 的二维方阵且满足 $M=N*N$;

(4)进行一次反扩散和反替换操作,采用逆扩散操作公式进行反扩散操作,在每次进行反扩散操作时利用步骤(2)得到的逆替换表 $k=f^{-1}(j)$ 进行反替换操作;

(5)利用离散化的 Arnold 变换公式以及所述的置乱过程对步骤(4)反扩散、反替换后的数据进行置乱操作;

(6)重复步骤(4)和(5),循环 l 轮;

(7)经过反扩散、反替换以及置乱后得到的数据块,即为明文数据,形成一维向量输出.

3　系统性能测试

首先利用所设计的混沌加密系统对电脑声卡发出的单频正弦信号进行了 Arnold 变换和 Logistic 映射,实现了混沌加密和解密,并比较了原始信号、加密信号和解密信号的波形,证明了其可行性;然后对一段 Rap 语音信号进行了加解密的实验测量,获得了比较满意的加密效果和解密一致性,证明混沌加密算法的 DSP 实现具有较高的安全性.

图 4(a)给出 10 Hz 单频正弦信号在加密前后的信号波形对比,可以看出加密后的信号和原始信号的完全不同,显示出杂乱无章的分布,根本无法辨别其中包含的正弦信号的信息,显示出本算法具有高安全性. 图 4(b)给出了解密波形与原始信号的对比,可以看出解密后的信号是一个单频正弦波,解密后的信号和原始信号基本一致,这进一步证明了本算法在加解密中具有良好的一致性.

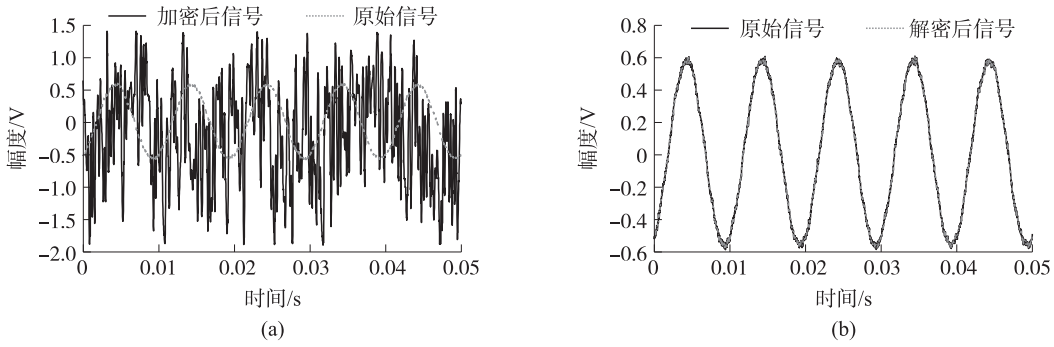

图 4　(a)单频正弦信号和加密信号,(b)单频正弦信号和解密信号

Fig. 4　Comparison of Single-frequency sinusoidal signal with (a) the chaotic encrypted signal and (b) the decrypt signal

图 5 给出 Rap 语音信号的原始波形和加解密后的波形及其频谱分布. 图 5(a)中的原始语音波形是多频信号的叠加,且在不同时刻显示出不同幅度的包络分布. 其频谱分析的结果如图 5(b)所示,可以看出信号频率主要集中在 500 ~ 8 000 Hz 之间,在 1 160、1 760、2 350、3 520、4 700、5 870 和 7 230 Hz 等频率周围形成明显的信号峰. 加密语音信号如图 5(c)所示,它和原始语音信号显示出完全不同的分布特性,没有变化的信号包络和幅度的变化,从其波形中根本无法分辨出 Rap 语音的变化规律. 如图 5(d)所示加密语音信号的频谱在 1 kHz 整数倍的频率上显示了几个尖锐的频率点,而其他频率的信号很小. 通过信号解密后的信号波形和频谱如图 5(e)和 5(f)所示,其形状和原始音频信号基本一致,同时其频谱在频率点和幅度上也基本相同. 另外通过耳机输出加密前和解密后的语音信号,人耳所听到的声音在音质、音高和音准等方面也基本相同. 通过实际 Rap 语音信号的实验测试,进一步证明了可逆二维 Arnold 变换和改进的 Logistic 映射算法在语音加密处理上的安全性和准确性.

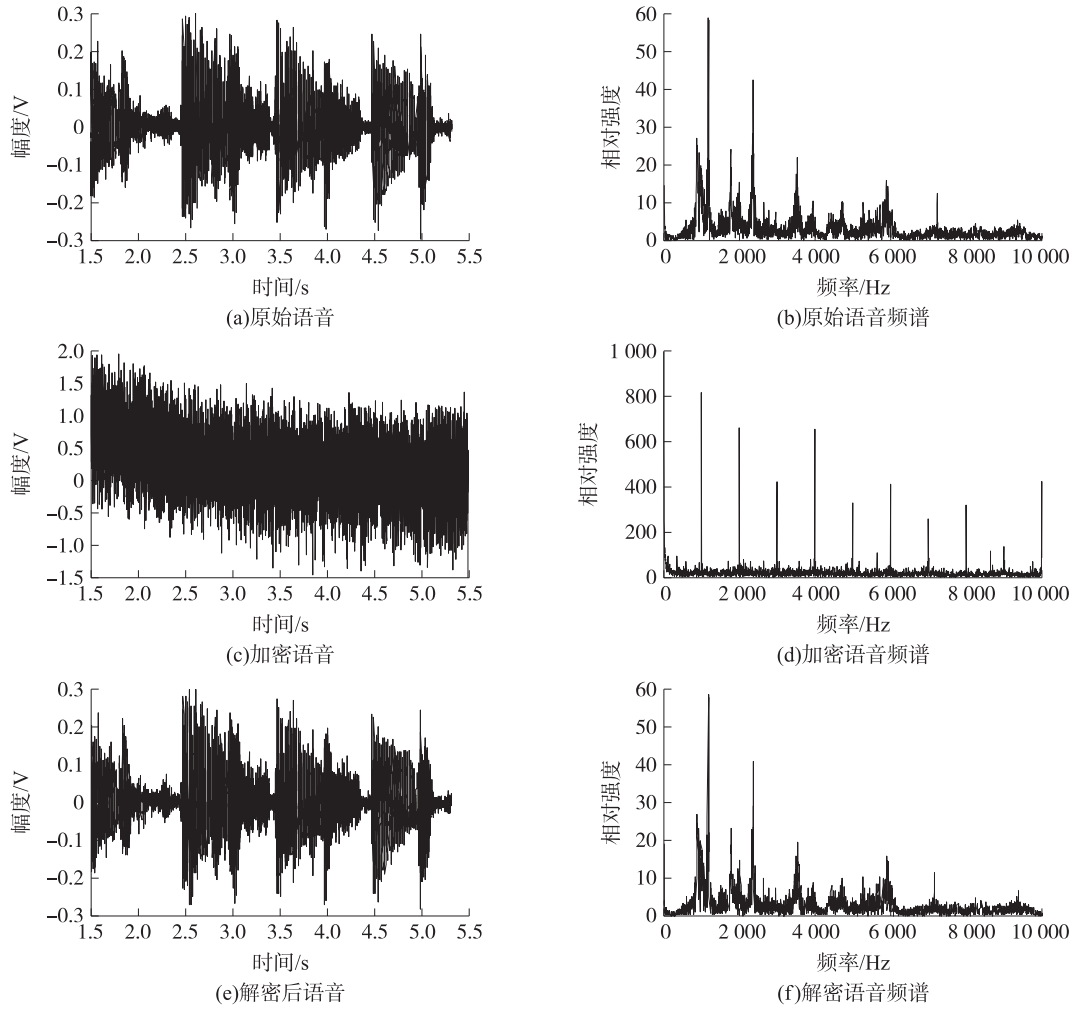

图 5　Rap 语音信号的原始波形(a)和频谱(b),Rap 语音信号加密后的波形(c)和频谱(d),Rap 语音信号解密后的波形(e)和频谱(f)

Fig. 5　Original waveform of the rap voice (a) and the spectrum (b), the encrypted waveform of the rap voice (c) and the spectrum (d), the decrypt waveform of the rap voice (e) and the spectrum (f)

4　结论

本文针对语音通信中的安全性问题,基于可逆二维 Arnold 变换和改进的 Logistic 映射加密算法,提出了一种改进的语音加解密混沌算法来提高了语音加密的安全性,并利用 DSP 处理器芯片 TMS320VC5509A 设计了一种具有语音信号采集、加密、解密和播放等功能的实验系统,对单频和 Rap 语音信号进行了性能测试和频谱分析,结果证明加密后的语音信号和原始信号看不出任何相关性,反映算法具有良好的安全性,同时解密后的信号在波形和频谱方面和原始信号基本一致,体现了算法的准确性. 本研究为语音通信中信号的加解密提供了一种安全高效的新技术.

[参考文献]

[1]　陈诚,曹秀英,帅富强. 数字跳频通信设备关键技术的研究与发现[J]. 南京师范大学学报:工程技术版,2007,7(4):80-83.

[2]　樊雷. IP 语音混沌加密算法研究[D]. 南京:南京理工大学自动化学院,2004.

[3]　侯爽. 语音加密算法及其在网络通信系统中的应用研究[D]. 南京:南京理工大学自动化学院,2007.

[4]　Goldburg B, Sridharan S, Dawson E. On the use of a frequency domain vector codebook for the cryptanalysis of analog speech scramblers[J]. IEEE International Symposium on Circuits and Systems, 1991, 1: 328-331.

[5] Cox R V,Bock D E,Bauer K B,et al. The analog voice privacy system[J]. AT&T Technical Journal,1987,66(1):119-131.
[6] 田丽平. 基于混沌复合映射的语音信号流安全通信仿真实现[J]. 计算机与现代化,2007(2):97-98.
[7] 魏建香,罗军舟. 基于哥德尔 β 函数的数据加密[J]. 南京师范大学学报:工程技术版,2002,2(1):14-17.
[8] 刘爱华,陈钧,解芳. 数据库敏感数据加密算法的研究与改进[J]. 南京师范大学学报:工程技术版,2012,12(3):68-70.
[9] Kocarev L,Jakimoski G,Stojanovski T,et al. From chaotic maps to encryption schemes[J]. IEEE International Symposium on Circuits and Systems,1998,4:514-517.
[10] 关新平,范正平,陈彩莲,等. 混沌控制及其在保密通信中的应用[M]. 北京:国防工业出版社,2002.
[11] Cuomo K M, Oppenheim A V, Strogatz S H. Synchronization of Lorenz-based chaotic circuits with applications to communications[J]. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 1993, 40: 626-633.
[12] Shannon C E. Communication theory of secrecy system[J]. Bell System Technical,1949,28(4):656-715.
[13] 樊雷,茅耀武,孙金生. 一种结合猫映射与 Logistic 映射的语音加密算法[J]. 控制与决策,2004,19(10):1 167-1 174.
[14] Dachselt F,Kelber K,Schwarz W,et al. Chaotic versus classical strean ciphers-a comparative study[C]//Proceedings of the 1998 IEEE International Symposium on Circuits and Systems. New York:IEEE,1998,4:518-521.
[15] Froyland J. Introduction to Chaos and Coherence[M]. London:Institute of Physics Publishing Ltd. ,1992.
[16] Jakimoski G,Kocarev L. Chaos and cryptography:block encryption ciphers based on chaotic maps[J]. IEEE Transactions on Circuits and Systems I:Fundamental Theory and Applications,2001,48(2):163-169.
[17] Texas Instruments. TMS320C55x DSP Mnemonic Instruction Set Reference Guide[M]. Texas:Texas Instruments,2000.
[18] 孟勃,朱明. 基于 McBSP 实现 DSP 与串行 Flash 之间的接口通讯[J]. 电子器件,2006,29(3):921-924.
[19] 顾学乔,李杰,徐寅林. DSP 与 PC 机的高速数据传输接口设计与实现[J]. 南京师范大学学报:工程技术版,2009,9(3):73-76.

[责任编辑:顾晓天]