

音频信号高速率采样中混沌实时加密的实现

杨 健, 王光义

(杭州电子科技大学 电子信息学院, 浙江 杭州 310018)

摘 要: 通过对音频信号高采样率采样过程中实时加密的研究, 提出了一种结合异或运算和循环移位操作的双重置乱混沌加密算法, 对高采样率音频信号进行加密和信息掩盖. 加密序列和循环移位序列均由混沌系统产生, 整个过程在数字信号处理器(DSP)平台进行了验证. 此方法运算速度快, 安全性高, 易于在嵌入式系统中进行应用.

关键词: 高采样率; 音频信号; 混沌加密; 数字信号处理器

中图分类号: TP37

文献标识码: A

文章编号: 1000-7180(2012)04-0062-05

The Realization of Chaos Real-time Encryption in the Process of Audio Signal High Rate Sampling

YANG Jian, WANG Guang-yi

(College of Electronic Information, Hangzhou Electronic Science and Technology University, Hangzhou 310018, China)

Abstract: This paper proposes a kind of algorithm which combination of XOR and cyclic shift, a dual-scrambling chaotic encryption via researching the real-time encrypt in the process of audio signal high rate sampling, to encrypt and cover the information of high sampling rate audio signal. Encryption sequence and cyclic shift sequence are generated by chaotic system; the whole process was verified in the digital signal processor (DSP) platform. This method is computing speed and high security, so it can be easily used in embedded systems.

Key words: high sampling rate; audio signal; chaotic encryption; digital signal processor

1 引言

针对多媒体信息的加密方法研究逐渐增多, 其中音频加密是一个研究的重点. 许多研究将传统的算法, 例如 AES 分组加密算法运用到音频加密中^[1], 但由于运算复杂耗时等原因, 该类算法在低采样率^[2] (例如 8 kHz 采样率) 语音加密中效果良好, 却难以在音频信号高采样率^[3] (例如 44.1 kHz, 48 kHz) 采集过程中进行实时加密, 否则将产生严重的信息丢失. 因此, 如何实现一种快速且安全性高的适合在音频高采样率采集过程中进行实时加密的算法是亟待解决的问题.

混沌是非线性动力系统中一种确定性的, 类似随机的过程^[4], 具有遍历性、非周期性、连续宽带频谱、似噪声的特性, 使其在密码学研究中得到了广泛

应用. 在音频加密运用中, 已有学者将其用于低采样率语音信号的实时加密^[5], 由于高采样率音频的信号高冗余性^[6], 仅通过混沌加密后的音频信号仍有大量音频包络未被破坏, 还原后还可分辨出原始音频. 本文根据大量实验验证, 提出了一种结合混沌异或加密和混沌循环移位的加密置乱算法, 对高采样率音频信号进行实时加密, 并通过 DSP 系统验证了该算法. 该算法适合于嵌入式系统中以高采样率采集加密音频信号或者版权公司对音频信号进行采集加密存储等领域的运用.

2 一个改进的三阶混沌系统及 DSP 实现

根据文献^[7]我们提出了一个改进的三阶混沌系统:

收稿日期: 2011-07-28; 修回日期: 2011-09-19

基金项目: 国家自然科学基金资助项目(60971046), 浙江省研究生创新科研资助项目(GK100202003)

$$\begin{cases} \dot{x} = a(y-x) + z \\ \dot{y} = (c-a)x - cxz \\ \dot{z} = -bz + xy \end{cases} \quad (1)$$

当 $a=2.1, b=0.6, c=9$ 时,用 MATLAB 仿真得到的混沌吸引子如图 1 所示。

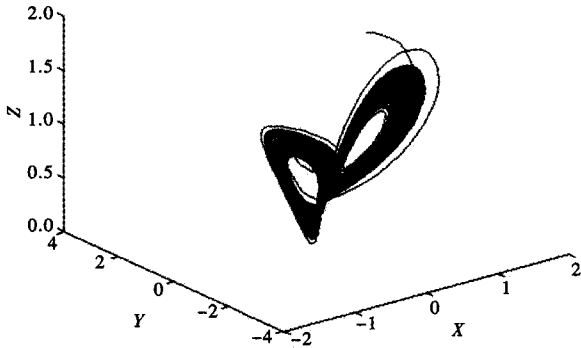


图 1 混沌吸引子图

由图 1 可以看出此时系统处于混沌状态^[7]。为了能够通过此系统抽取混沌序列,用于 DSP 中对音频信号加密,必须将该连续系统进行离散化处理。常用的离散化方法包括:(1)差商逼近法;(2)数值积分法;(3)Taylor 展开法。本文采用差商逼近法,即用适当差商逼近导数值,使式(1)离散化^[8]。原理式为

$$\begin{cases} \dot{x} = f(x) = \lim_{\tau \rightarrow 0} \frac{x_n - x_{n-1}}{\tau} \\ x_n = x_{n-1} + \tau f(x_{n-1}) \end{cases} \quad (2)$$

式中, τ 为量化间隔。根据式(2),对混沌系统进行离散化后得

$$\begin{cases} x(n) = \tau(ay(n-1)x(n-1) + z(n-1)) + x(n-1) \\ y(n) = \tau((c-a)x(n-1) - cx(n-1) + z(n-1)) + y(n-1) \\ z(n) = \tau(-bz(n-1) + x(n-1)y(n-1)) + z(n-1) \end{cases} \quad (3)$$

这里 τ 取 0.02。在 DSP 中将式(3)作为程序循环体,进行迭代抽取序列。具体的抽取方式如下:异或加密序列选择 $x(n)$ 作为抽取序列的迭代式,每迭代一次,抽取其中的第二位,迭代十六次后得到一个十六位的序列,用于与音频码流的异或加密运算。循环移位序列抽取了式子 $y(n)$ 每次迭代值中的低四位。我们使用示波器观察了通过 DSP 运算得到的序列波形图,如图 2 所示。

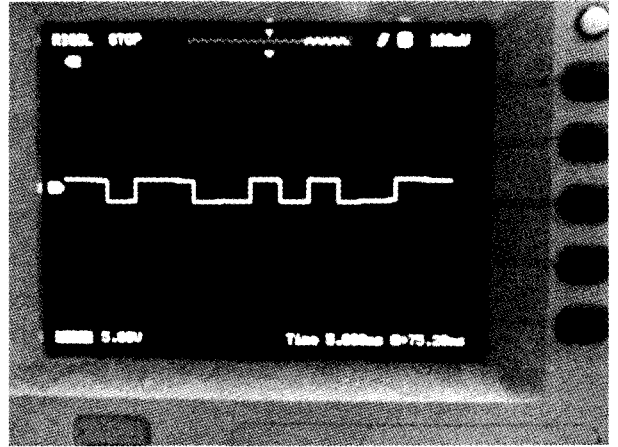


图 2 通过示波器观察到的实际序列波形图

3 加密算法及在 DSP 中的实现

本文的运用背景为对音频信号高采样率采样过程中的实时加密,系统对于时间敏感,稍长的延时将导致采样音频性能变坏。因此,本文提出的算法使用异或和循环移位运算的组合,运算速度快,适合于嵌入式系统中运用。具体算法如下所示。

3.1 加密端算法

加密过程表示成

$$c = c_{(1)}c_{(2)}\cdots = f_{y(1)}[e_{x(1)}(p_{(1)})]f_{y(2)}[e_{x(2)}(p_{(2)})]\cdots \quad (4)$$

式中, $p = \{p_1 p_2 \cdots\}$ 是待加密的音频码流, $x = \{x_1, x_2 \cdots\}$ 是用于异或加密的混沌序列, $y = \{y_1, y_2\}$ 是用于循环移位的混沌序列。函数 $e_{x(t)}$ 表示将音频码流 $p(t)$ 和混沌序列 $x(t)$ 进行异或运算,函数 $f_{y(t)}$ 表示将异或加密后的码流进行循环移位 $y(t)$ 位, $c = \{c_1 c_2 \cdots\}$ 是加密后的码流。具体算法如下:

将音频信号以 48 kHz 的高采样率进行采样,得到 16 位的音频码流 $p(t)$ 。第一步,通过混沌系统抽取一组 16 位混沌序列 $x(t)$ 同音频码流 $p(t)$ 进行异或加密运算,得到加密后的码流。第二步,从混沌系统抽取一组 4 位的混沌序列 $y(t)$,将加密后的码流进行循环移位 $y(t)$ 位的运算。通过这两个步骤,得到了加密置乱后的音频码流 $c(t)$,算法结构如图 3 所示。

在实验中,通过使用 AIC23 模块以 48 kHz 的 MP3 音质高采样率采集由计算机输入的一段 0.3~3 kHz 音频,采集后所有加密、移位运算在 DSP (TMS320VC5509A) 中完成。通过开发环境 CCS3.3 的图形分析工具(Graphical Display)采集波形,并

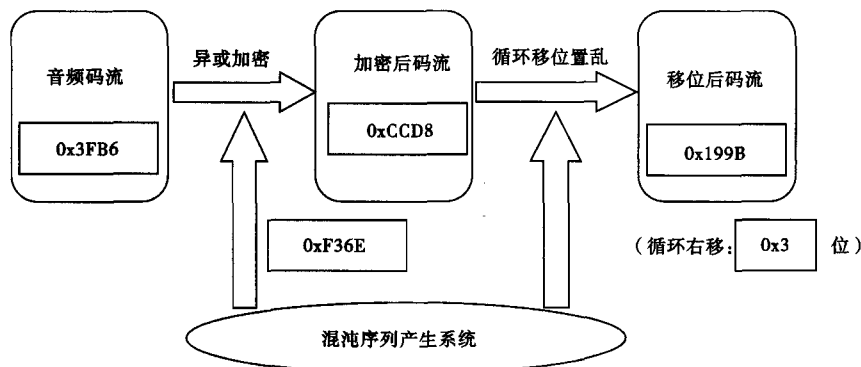


图3 加密算法图

进行分析. 原始波形和混沌序列异或加密后的波形对比如图4所示(波形的横坐标是采样点,纵坐标是该点的量化电平值,下同).

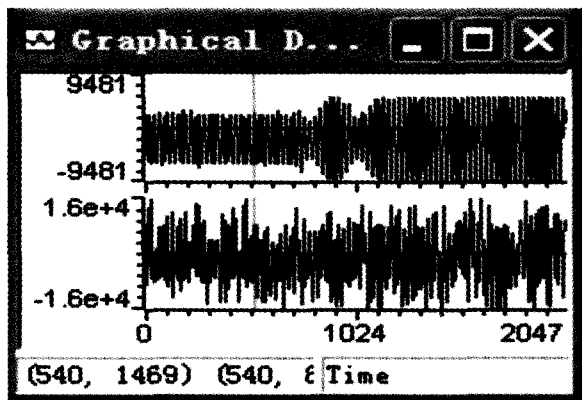


图4 原始波形(上)和异或加密后波形对比(下)

从图4可以看到,在原始音频信号密集的包络处,仅使用一次异或加密后未能有效破坏原始包络的分布,将加密后的码流通过AIC23模块还原为音频,可以听到杂音掩盖下的微弱原始音频信号. 因此经过异或加密虽然音频序列已经置乱,但由于高采样率音频信号的高冗余特性,仍能分辨原始音频. 为了起到有效的保密效果,需要对加密后音频序列进行进一步置乱以破坏原始包络.

循环移位后的波形与原始音频波形对比如图5所示,由图5可以看出,加密移位后的波形将原始的包络完全破坏,将此时码流还原为音频,听到的是杂乱的噪声,无法分辨原始音频信号. 至此,完成了对高采样率音频信号的实时加密运算.

3.2 解密端算法

解密过程表示为

$$p = p_{(1)} p_{(2)} \cdots = g_{y(1)} [e_{x(1)} (c_{(1)})] g_{y(2)} [e_{x(2)} (c_{(2)})] \cdots \quad (5)$$

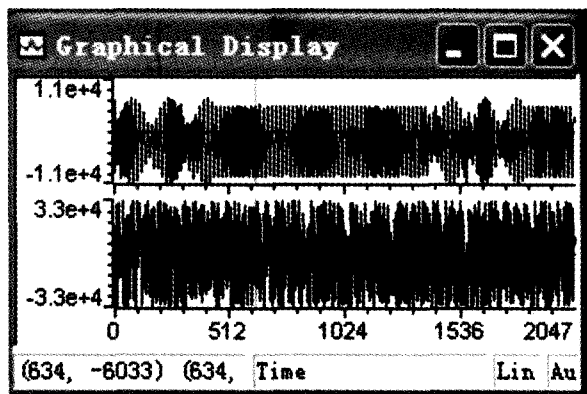


图5 原始波形(上)与循环移位后波形对比(下)

式中,函数 $g_{y(t)}$ 表示将音频码流按与函数 $f_{y(t)}$ 相反的方向循环移位 $y(t)$ 位.

解密端通过使用与加密端完全相反的逆运算进行数据的解密,解密成功的关键在于使用的混沌系统与加密端是完全相同且同步的. 由于本文仅限说明该算法的一般过程,不涉及传输,因此同步性问题将在以后的研究中进一步考虑. 解密首先将音频码流进行与加密端反向的循环移位,然后再将移位后的音频码流与加密端相同的混沌序列进行异或解密运算,得到还原的音频信号. 如图6所示.

实验验证了该算法能够进行正确的解密. 原始波形与反向循环移位后的波形对比如图7所示,可以看出,经过反向循环移位已经基本恢复了原始音频信号的包络分布. 再经过一次异或解密后即恢复出原始音频信号,原始音频波形和完全解密后的音频波形对比如图8所示. 解密后的音频恢复了原始音频的包络,通过回放音频信号,听到了清晰的音频,达到了解密的目的.

4 性能分析

4.1 密钥空间分析

该加密算法引入了系统参数 a 、 b 、 c , 利用

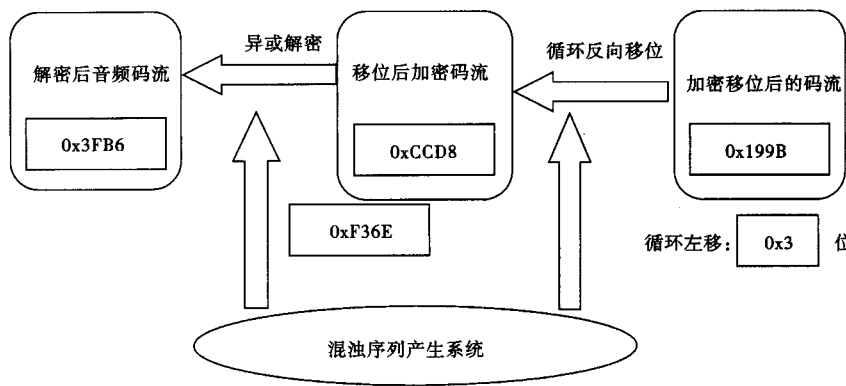


图 6 解密算法图

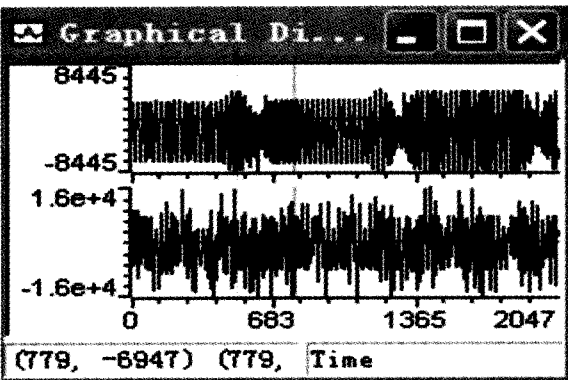


图 7 原始音频(上)与反向移位后波形对比(下)

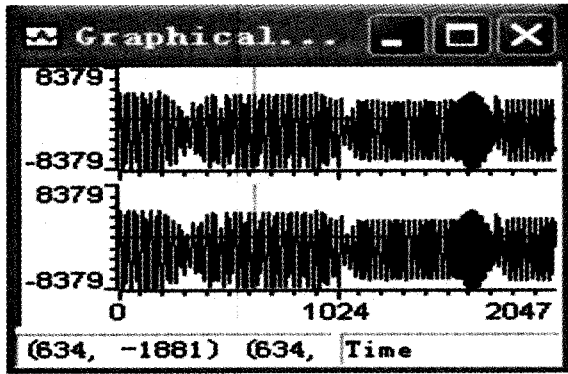


图 8 原始音频(上)与解密后音频波形对比(下)

MATLAB 对混沌方程(1)进行相关计算,确定使系统进入混沌状态的参数取值范围.需要说明的是,由于混沌系统有相当复杂的动力学特性,所以要确定出在整个实数域内使方程出现混沌的各个参数变化范围难度较大,同时考虑到密钥空间估计的目的在于能够说明其足以抵抗穷举攻击,因此我们考虑了这些参数的一部分变化范围,而实际的密钥空间将会更大.表 1 所示为各个参数变化范围.

其次,初值 $x(0),y(0),z(0)$ 的取值范围分别取 $[-4,2],[-2,3],[-0.5,2.5]$,另外考虑实验中所

表 1 各参数变化范围

参数名称	a	b	c
变化范围	2.1~2.8	0.6~0.9	9~30.1

使用的 DSP 芯片为 16 位定点 DSP,其运算精度为 $0.003\ 052\%^{[8]}$,此处取 10^{-6} . 综上,该系统的密钥空间约为

$$0.7 \times 10^6 \times 0.3 \times 10^6 \times 21.1 \times 10^6 \times 6 \times 10^6 \times 5 \times 10^6 \times 3 \times 10^6 \approx 3.98 \times 10^{38} \quad (6)$$

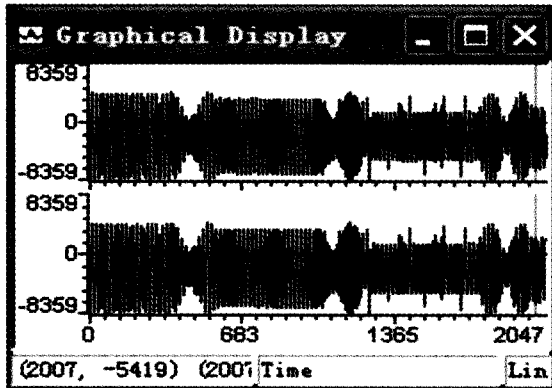
假设密码分析人员使用目前世界上运行速度最快的计算机以每秒千万亿次搜索密钥,仍然需要大约 3.9×10^{12} 年才能够穷举所用密钥. 所以,该算法能够很好的抵抗穷举攻击.

4.2 密钥敏感性分析

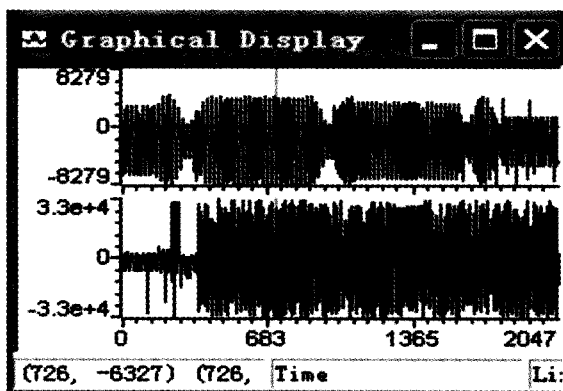
系统采用了混沌加密算法,而混沌具有较高的参数敏感性,因此,我们进行了密钥敏感性的测试. 如图 9 所示,给出了参数 c 在加密时取 30,解密时取 30(图 9(a)) 和 30.001(图 9(b)) 的波形对比图. 由波形对比可以看出,即使初值相差微小也无法正确解密原始音频信号,该系统具有较高的密钥敏感性.

5 结束语

本文提出了一种混沌在音频信号高采样率采集过程中实时加密的方案,并对该方案的安全性进行了分析和实验验证. 实验结果表明该方案具有良好的加密效果,且还原后的音频音质保留了原始音频的特性. 该方案的运算特点使其适合于嵌入式系统中音频高采样率采集过程中实时加密的运用. 实验在 DSP 平台进行了验证,通过一定的改造,该方案可方便地移植到 FPGA、ARM 等其他嵌入式平台,具有良好的通用性.



(a)原始音频(上)和 c 取 30 的解密波形(下)



(b)原始音频(上)和 c 取 30.001 的解密图(下)

图 9 密钥敏感性测试

参考文献:

- [1] 刘运毅,覃团发,倪皖荪,等. 基于 G. 729A 和 AES 的分组语音保密通信[J]. 南京大学学报:自然科学版, 2005,41(4):1-10.
- [2] 潘桐. G. 726 语音压缩算法在低码率下的改进与实现[J]. 微计算机应用, 2009,30(4):76-78.
- [3] 游鹏,季晓勇,卢鹏. 对 G. 723.1 高码率编码语音中进行压缩域信息隐藏的性能分析[J]. 计算机科学, 2008,35(5):194-195.
- [4] 罗启彬,张健. 混沌密钥序列的 DSP 实现算法研究[J]. 微电子学与计算机, 2009,26(2):44-46.
- [5] 盛苏英,陆国平,吴新华. 混沌语音实时保密通信研究[J]. 微电子学与计算机, 2008,25(3):84-86.
- [6] Annie Lang. Information processing perspective defining audio/video redundancy from a limited-capacity[J]. Communication Research, 1995(22): 86
- [7] Zhou Xiaobing, Zhang Jinfu, Jiang Murong. Passivity-based adaptive chaos control of a new 3D chaotic system with uncertain parameter[C]// Information Technology and Applications, 2009. IFITA '09. International Forum on. 2009(3):57-60.
- [8] 高颖. 定点 DSP 中运算精度的提高[J]. 电子工程师, 2001,27(9):3-4.

(上接第 61 页)

参考文献:

- [1] Dugad R, Ahuja N. A fast scheme for image size change in the compressed domain[J]. IEEE Transactions on Circuits System Video Technology, 2001, 11(4): 461-474.
- [2] Mukherjee J, Mitra S K. Image resizing in the compressed domain using subband DCT[J]. IEEE Transactions on Circuits System Video Technology, 2002, 12(7): 620-627.
- [3] Shu H T, Chau L P. An efficient arbitrary downsizing algorithm for video transcoding[J]. IEEE Transactions on Circuits System Video Technology, 2004, 14(6): 887-891.
- [4] Park H W, Park Y S, Oh S K. L/M-image folding in block DCT domain using symmetric convolution [J]. IEEE Trans. Image Process, 2003, 12(9): 1016-1034.
- [5] Tan Eeleng, Gan Woonseng, Wong Mengtong. Fast image resizing in discrete cosine transform domain

with relationship between DCT block and its sub-blocks[C] // 2010 International Conference, Audio Language and Image Processing (ICALIP). China: Shanghai, 2010: 1683-1687.

- [6] Avidan S, Shamir A. Seam carving for content-aware image resizing[J]. ACM Transactions on Graphics, 2007,26(3):10.
- [7] Han J W, Choi K S, Wang T S, et al. Wavelet based seam carving for content-aware image resizing[C]// Proc. of IEEE International Conference on Image Processing. Cairo, Egypt, 2009: 345-348.
- [8] 史海滨,朱光喜,喻莉,等. 一种基于预测频度的 AVS/H. 264 的快速 4x4 帧内预测模式选择算法[J]. 微电子学与计算机, 2007,24(8):8-10.

作者简介:

王 峰 女, (1984—), 硕士研究生. 研究方向为多媒体智能信息处理.

郑江滨 男, (1971—), 教授. 研究方向为语音图像处理与计算机视觉.