

基于改进混沌密码的音频信息隐藏算法研究

赵家弘¹, 尹 萍²

(1 北京航天光华电子技术有限公司(航天九院 200 厂), 北京 100039;

2 北京佰能电气技术有限公司, 北京 100096)

摘 要: 基于混沌密码理论, 提出一种新型加密方案. 首先利用 Arnold 猫映射和 3D-Lorenz 混沌系统, 通过改进算法产生混合混沌序列, 再将其与明文信息运算产生密文信息, 最后通过改进 LSB 信息隐藏算法将密文信息隐入音频载体. 合法用户通过理想信道得到密钥和加密流程即可通过逆运算安全获得明文信息. 经实验仿真证明, 改进后的混沌序列完全满足各项密码学特性, 整个系统能够安全、可靠地实现私密信息的网络传输.

关键词: 混沌密码; 信息隐藏; 音频信息处理; 网络通信

中图分类号: TN918.1

文献标识码: A

文章编号: 1000-7180(2013)05-0141-04

Research on Embedded Audio Information Hiding Algorithm Based on Improved Chaotic Password

ZHAO Jia-hong¹, YIN Ping²

(1 Beijing Aerospace Guanghua Electronics Technologies Limited Corporation(No. 200 Factory of CASC 9th Academy), Beijing 100039, China; 2 Beijing Bestpower Electrical Technology Limited Corporation, Beijing 100096, China)

Abstract: Based on the chaotic password theory, a new encryption method is brought forward. Firstly Arnold's cat mapping and 3D-Lorenz chaotic system are used by ameliorated algorithm to generate mixed chaotic sequences. Then the plaintext message is calculated with the sequences to generate the ciphertext message. Finally, the ciphertext is hided in audio carrier through improved LSB information hiding algorithm. The legal users can get the keys and the encryption workflow through the ideal channel. Then they can obtain the plaintext message in security by inverse operation. It is demonstrated by the simulation results that the improved chaotic sequences can completely meet the various cryptographic properties. And the whole system can realize the network transmission of private information safely and reliably.

Key words: chaotic password; information hiding; audio information processing; network communication

1 引言

随着计算机网络的快速发展和多媒体信息的广泛应用, 多媒体信息的网络通信日渐蓬勃. 由于数字信息具有可复制性, 随之出现了版权争端问题. 同时, 政府、企业、个人都在利用这一开放互连的公共信息网络平台, 构建各自的专用网络, 传递各自的私密信息. 这给人们带来方便快捷的同时, 也使得信息安全问题成为重中之重.

由于美国数据加密标准(DES)等传统加密方案

相继有被破解的案例, 目前国际上正在探讨一些非传统加密方案, 而借助混沌理论就是其中的一种主要方法. 英国数学家 Matthews 最早分析了 Logistic 混沌映射作为序列密钥流生成器时的的问题, 并对其做出改进^[1]. Biham 后来指出, 使用选择密文攻击可容易地对该系统解密, 并已知明文攻击复杂度为 238^[2]. 在国内, 韦军、杨吉云等还提出通过动态更新查询表实现加解密, 加快了运行速度^[3]. 但是直到目前, 混沌密码的研究整体上还处于起步阶段, 具有良好密码学特性的解决方案亟待探索.

本文设计出一套加解密解决方案,并将其嵌入音频信息隐藏算法.系统仿真实验验证,该方案具有良好的密码学特性.

2 系统原理分析与方案设计

2.1 基于混沌系统的加密算法原理

基于改进混沌密码的音频信息隐藏算法包括两个部分,即混沌加密系统和音频信息隐藏系统两部分,其中混沌加密系统总体设计方案如图 1 所示.在该方案中,混沌映射 f 表示所选的混沌系统,由它可以通过迭代算法产生一定的混沌序列,记为 x_i .然后,混沌序列作为驱动序列通过归一化算法,即编码 C 最终得到密钥流 k_i .图 1 中的初始化过程包括对混沌系统的初始条件、迭代次数以及用于组合编码的顺序表等,这些输入实质上都被定义为系统工作密钥.

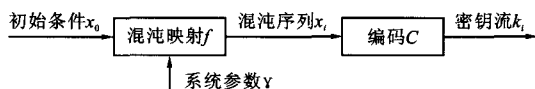


图 1 混沌加密系统设计方案示意图

利用混沌序列伪随机性等特性设计加密算法,首先要确定具有良好密码学特性的混沌系统.混沌系统的选择既要使所产生的序列符合各项密码学指标,还要对混沌系统本身提出一些指标要求,如 Lyapounov 指数、信息熵、参数敏感性、序列分布的随机性、周期性等^[4].经过研究,选择常用于混沌序列发生器的 3D-Lorenz 混沌系统和 Arnold 映射展开讨论.

3D-Lorenz 系统的动力学方程为:

$$\begin{cases} x_{n+1} = \sigma(y_n - x_n) \\ y_{n+1} = \gamma x_n - z_n x_n - y_n \\ z_{n+1} = x_n y_n - \beta z_n \end{cases} \quad (1)$$

式中,系统参数 σ, β, γ 的典型值分别为 $\sigma = 10$ 、 $\beta = 28$ 、 $\gamma = \frac{8}{3}$,在 σ 和 β 保持不变, $\gamma > 24.74$ 时,系统进入混沌态.显然这里是采用了三维的 Lorenz 变换^[4].在应用 3D-Lorenz 变换时,通常采用更加简单易行且满足性能指标要求的变换方程,如式(2)所示.

$$\begin{cases} x_{n+1} = x_n y_n - z_n \\ y_{n+1} = x_n \\ z_{n+1} = y_n \end{cases} \quad (2)$$

Arnold 映射又叫猫映射,其矩阵形式方程如下所示^[5]:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & k \end{bmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 = C \begin{pmatrix} x_n \\ y_n \end{pmatrix} \bmod 1 \quad (3)$$

其中,系统参数 k 一般取 2,“mod1”表示只取小数部分,即 $x \bmod 1 = x - [x]$,因此 (x_n, y_n) 的相空间限制在单位正方形 $[0, 1] \times [0, 1]$ 内.此外,上式还定义了 C ,注意到行列式 $|C| = 1$,因此 Arnold 映射是一个保面积映射(没有吸引子).

根据 Kerckhoffs 原则不难发现,从密钥空间上看,Arnold 映射初次迭代后的两个序列输出值和 3D-Lorenz 系统初次迭代后的三个序列输出值都可以作为系统密钥设法安全传送给合法用户,故分别采用一种系统时密钥空间最大是 3 维.而将两混沌序列“混合”时需要用到的 2 个加权系数,加上两系统输出序列总共的 5 个密钥,可将密钥空间增至 7 维,这使得系统的安全性大大提高^[6].于是基于采用混合混沌系统的创新加密方案,给定初始条件和系统参数,即可得到所需的混沌密钥流.

2.2 基于混沌密码的音频信息隐藏算法原理

采取类似于混沌掩盖的算法,将混沌密钥流与需要进行加密的明文信息流直接按位异或,即可产生相应的密文输出^[7].输出密文信息后,需要通过信息隐藏技术将其隐入一定的音频载体,其一般框架如图 2 所示.

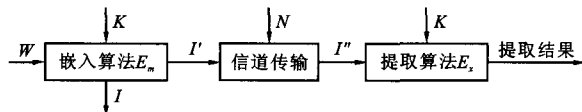


图 2 信息隐藏技术的一般框架

其中,秘密信息 W 与密钥 K 相结合,通过嵌入算法将 E_m 隐藏到原始信息 I 中,形成含有秘密信息的载体 I' , I' 与 I 应非常相似,不会引起他人的怀疑.一般情况下, I' 在无噪信道中传输,但在一些特殊应用场合也会考虑噪声 N 对载体数据的干扰,即 I' 变为 I'' .对 I'' 应用提取算法 E_x ,可以正确提取出秘密信息 K .

根据信息隐藏技术的一般框架,将音频数字化后,采取最不重要位(LSB)法将密文信息与数字音频信息的 LSB 作运算,而不致人耳分辨出混合后音频与原始音频的差别.为提高它的安全性,对 LSB 方法中的位替换运算改为加减运算,将 0、1 数据流变换为 -1、1 数据流,这样 LSB 的每一位势必会改变,故改进后的 LSB 方法会比传统方法可靠性更好^[8].

通过理想信道传输,合法用户可得到已隐藏数

据的音频文件,再根据先前秘密得到的密钥,采取与加密流程相反的操作,即可得到隐藏在音频信息中的秘密信息。

3 算法与软件设计

3.1 改进混沌伪随机序列生成算法设计

按照预设方案,在 Matlab 7.5.0(R2007b)仿真平台上进行算法实现与计算机仿真。根据式(2),首先对 3D-Lorenz 系统进行初始化,给定系统初始条件,定义变量 x, y, z , 对其赋初值 $x = 0.5, y = 0.5, z = -1$ 。然后根据初始条件和动力学方程进行迭代运算,计算出迭代 5000 次后的系统状态 (x, y, z) 。这时 (x, y, z) 的不可预测性已经很好了,因为迭代多次后,若初始条件有微小的改变,都足以使得 (x, y, z) 产生巨大的变化,这正是采用混沌序列的优异性所在。之后对 (x, y, z) 做进一步迭代,将此后迭代 20000 次过程中的每一个数字都按顺序存放在三维数组中,生成 3D-Lorenz 混沌序列,将结果保存至文件中。

其次根据式(3)对 Arnold 系统进行初始化,定义变量 x, y 并赋初值 $x = 0, y = 1/\sqrt{2}$, 给定系统参数 $k=2$, 用同样的方式生成 Arnold 混沌序列,如图 3 左图所示。

最后,根据预设方案将两混沌序列进行加权组合,生成混合混沌序列,并使用标准化算法使生成的随机序列从杂乱无章的小数变为一系列 $[0, 255]$ 之间的随机数字,具体算法如下:

$$\text{key} = \text{mod}(\text{round}(100000 \times 255 \times (x - \min(x)) / (\max(x) - \min(x))), 256) \quad (4)$$

其中, x 即之前产生的混沌序列。接下来就可以按方案生成密文了,如图 3 右图所示。

能够获得该音频的采样频率和量化位数。然后测量密文信息的长度,得到它的行、列数分别为 m, n 。将密文信息的 0、1 数据流变换为 -1、1 数据流,之后将密文信息隐藏在音频信息的第 $m \times n + 1$ 位至第 $2 \times m \times n$ 位的位置,显然可以发现利用这种算法,音频信息数字化后的长度必须大于密文信息长度的 2 倍,这样可以使密文信息不隐藏在音频信号开头,而是隐藏在中间的某一段,提高了信息隐蔽性。

这里可以设定一个密钥,即定义 LSB 的位数 N , 将密文信息与音频指定段数据的小数点后第 N 位相叠加。这不仅提高了信息隐藏的隐蔽性,同时也将加密算法的密钥空间增至 8 维。最后,将隐藏后的数据以原采样频率和量化位数写入新文件并播放,即可观察隐藏效果。

3.2.2 信息提取及解密算法设计

由 Kerckhoffs 原则,在解密程序设计之前,首先假定合法用户已经通过秘密途径得到所有正确的密钥,然后假定加密算法及加密前和加密后的音频文件都是对外公开的,即用户可以很容易通过网络等一些途径获得需要的音频文件。得到必要的密钥和音频文件后,首先读入两音频文件并得到其数据流,通过对照相减即可得到偏差信号,也就是嵌入的密文信息。之后按照加密算法的逆过程进行解密计算即可完成解密过程。

3.3 系统可视化界面设计

为让算法更加友好,利用 Matlab 图形用户界面 (GUI) 提供的强大可视化功能编写系统界面,通过在界面中设置功能按钮及状态显示框实现相应功能。用户在操作过程中,首先要选择加密所使用的混沌系统,不同的混沌系统产生的混沌序列性能上将存在一定差异。然后需要输入音频载体文件名、明文文件名、LSB 的设定位数。最后点击下方的按钮即可实现加密、解密功能,还可根据需要进行绘图,观察混沌系统输出序列状态。

4 系统性能测试与安全性分析

4.1 混沌序列伪随机性测试

为验证混沌优化搜索算法可以遍历优化变量的取值区间,且能够搜索到全局最优解,对混沌系统的混沌特性进行分析。这里以 Arnold 猫映射为例,对系统赋初值 $(1, 1)$, 即可得到序列随迭代次数 k 的变化在坐标系中的所有取值如图 4 所示。经测试表明此系统可以通过迭代及“放大”遍历优化变量的取值范围,并能产生分布均匀、伪随机性良好的混沌序列。

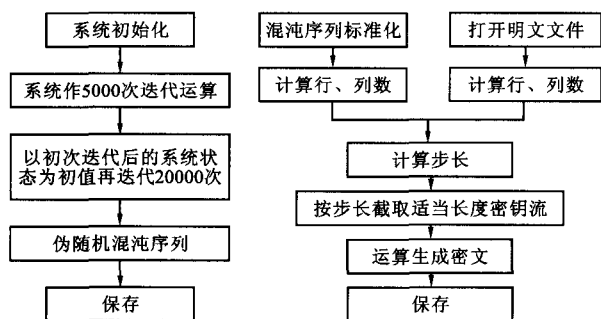


图3 基于混沌序列的密文生成算法流程图

3.2 基于改进混沌密码的音频信息隐藏算法设计

3.2.1 信息隐藏算法设计

首先将音频文件数字化,得到音频数据流,同时

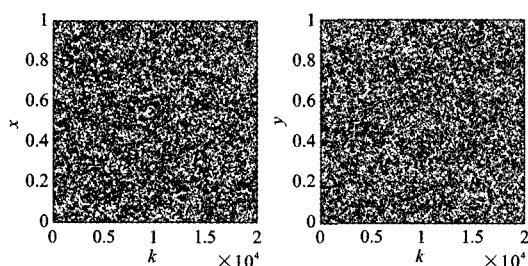


图4 Arnold映射 x 序列、 y 序列迭代取值示意图

4.2 扰动密钥流游程分析

为进一步检验 0、1 密钥流的随机性能,需要分析其主要统计特性是否与理想的“随机”序列的统计特性相一致。目前,公认的衡量标准是 Golomb 提出的三个随机性公设^[9]。

实验表明,本方案生成密钥流的伪随机性能优于根据 Golomb 公设计算得出的上限值,并位于美国 FIPS-1402 标准所规定的范围内。由此可以得出,所设计的算法能产生随机性能较为优异的混沌序列。采用本文改进的混沌系统,密钥空间可达到 $(10^{14})^8 = 10^{112}$,远远优于系统要求。

4.3 相关性分析

实验测试中,对流行乐曲片段进行实验,此处只对左声道进行信息隐藏,右声道无变化。载体信号为双声道高保真音乐,采样频率为 44.1kHz,量化精度 16 比特,位速 1411kbps。

下面分别对隐藏前后左声道、隐藏前左右声道和隐藏后左右声道的相关性进行计算:

(1)隐藏前后左声道的相关性:

$$C_1 = 0.999999999998993;$$

(2)隐藏前左右声道的相关性:

$$C_2 = 0.1809086763238098;$$

(3)隐藏后左右声道的相关性:

$$C_3 = 0.1809086764200786.$$

C_1 接近 1 说明隐藏信号前后左声道信息几乎无变化。 C_2 和 C_3 相等说明信息隐藏前后音频统计特性几乎不发生改变,故攻击者在进行攻击时很难通过对音频统计特性的分析找到破绽,系统具有很好的安全性。图 5 为信息隐藏前后音频左声道的波形。

通过以上分析,可以得出混沌密码系统对初始密钥表现为极强的依赖性,说明混沌系统用于保密通讯效果较好,能够对以音频信号为载体进行有效的文本信息加密。并且,同样在经过参数的最优调节后,采用混合混沌系统加密要比单独采用一种混沌系统性能优越。

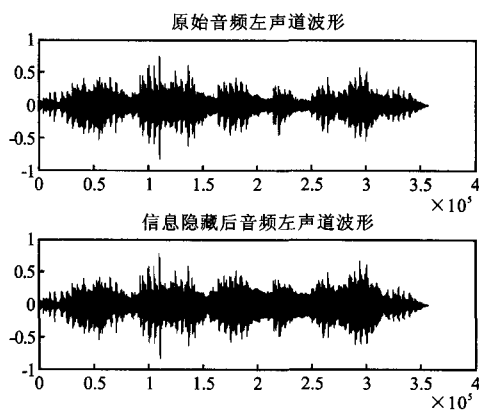


图5 信息隐藏前后音频左声道波形对比示意图

5 结束语

本文利用混沌序列伪随机性好等特点,设计了一种基于改进混沌密码的音频信息隐藏系统。通过将性能优良的两混沌系统按密钥进行混合运算,一方面融合了两系统的优势,提高了序列的伪随机性;另一方面使密钥空间大幅增加,大大提高了系统安全性。该算法仍有很大空间值得继续探索。比如假设密钥已通过理想信道传递给合法用户,这一传输细节需要保密通信技术得以保证。本算法只对无损音频载体进行了信息隐藏,若选择压缩音频甚至视频作为载体,则需要对改进型 LSB 法做进一步探讨。此外,还可结合人耳生理特点提高算法隐蔽性等。

参考文献:

- [1] Matthew R. On the derivation of a 'chaotic' encryption algorithm[J]. Cryptologia, 1989, 13(1): 29-42.
- [2] Biham E. Cryptanalysis of the chaotic - map cryptosystem[C]// Proc Advances in Cryptology, EURO-CRYPT '91, Berlin, Germany: IEEE, 1991: 532-534.
- [3] 韦军, 杨吉云. 对一个混沌密码模型的分析[J]. 通信学报, 2008, 29(9): 134-140.
- [4] 周黎晖, 彭召旺. 混沌加密系统的保密性能[J]. 上海交通大学学报, 2001, 35(1): 133-138.
- [5] 魏明, 蔡延光. 一种基于混沌领域搜索的自适应遗传算法[J]. 计算机应用研究, 2009, 2(2): 148-149.
- [6] 廖晓峰. 混沌密码学原理及其应用[M]. 北京: 科学出版社, 2009.
- [7] Jim Chou, Kannan Ramchandrad, Antonio Ortega. Next generation techniques for robust and imperceptible audio data hiding[C]// Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing, Piscataway, NJ, USA: IEEE, 2001: 1349-1352.

(下转第 148 页)

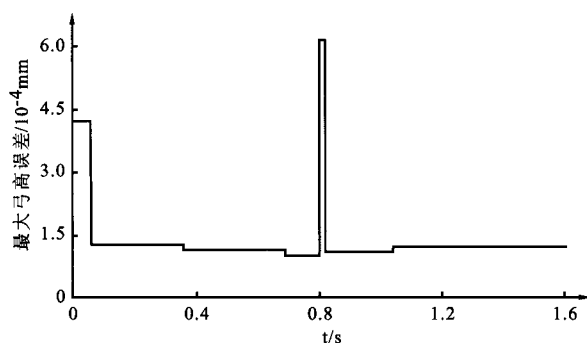


图2 最大弓高误差的仿真曲线

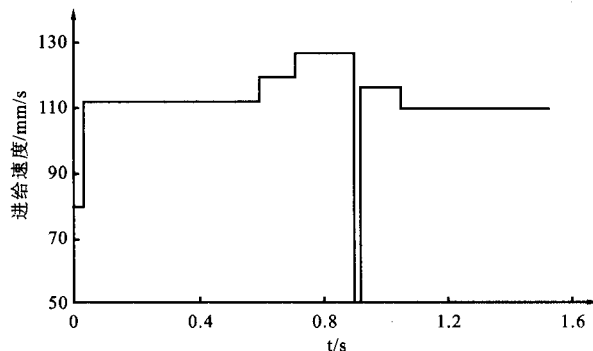


图3 汽轮机叶片加工进给速度的仿真曲线

速度可以根据叶片曲线不同位置的曲率变化加以调节,同时进给速度的变化幅度也能够给有效地提高,从而使加工效率得到了极大的提高。

5 结束语

将粒子群算法引入到了 NURBS 曲线的插补控制算法中,使汽轮机叶片的加工精度得到了极大的

提高,该控制算法不仅能够保证叶片的加工精度要求,而且能够灵活地调节进给速度,从而使叶片的加工效率得到提高。进而降低了加工机床的振动,对于汽轮机叶片高精度加工具有较好的借鉴作用。

参考文献:

- [1] 韩庆瑶,唐月夏,乐英. 汽轮机叶片数控加工的直接插补算法研究[J]. 机床与液压, 2010, 38(9):26-29.
- [2] 乐英. 提高汽轮机叶片加工效率的方法[J]. 汽轮机技术, 2012, 54(3):234-238.
- [3] 隋永枫,孙义冈,叶钟,等. 汽轮机叶片改型及三维气动优化设计[J]. 热力透平, 2011, 40(1):28-32.
- [4] 隋永枫,孙义冈,丁旭东,等. 不调频叶片设计改型研究[J]. 热力透平. 2010, 39(1):19-21.
- [5] 杨敏超,孙苏亚. 涡轮榫头榫槽的结构优化设计[J]. 航空动力学报, 2010, 25(8):1876-1882.
- [6] 李静,高正红,黄江涛,等. 基于分布式粒子群算法的翼型优化设计[J]. 空气动力学学报, 2011, 29(4): 464-469.
- [7] 侯磊. 基于多目标粒子群算法的船舶主尺度优化设计研究[J]. 船舶力学, 2011, 15(7):784-790.

作者简介:

郭旭敏 男,(1987—),硕士研究生,讲师. 研究方向为数据挖掘.

张月琴 女,(1963—),硕士研究生,教授. 研究方向为数据挖掘.

冯珊珊 女,(1986—),硕士研究生. 研究方向为数据挖掘.

(上接第 144 页)

- [8] 饶华一,陈铭,张茹,等. 信息隐藏和隐写分析综述 [C]//2007 北京地区高校研究生学术交流会通信与信息技术会议论文集(上册),中国电子学会信息论分会,北京:2008: 138-141.
- [9] 金晨辉,杨阳,祁传达. 对混沌序列密码的相关密钥

攻击[J]. 电子与信息学报, 2006(3): 410-414.

作者简介:

赵家弘 男,(1986—),硕士,助理工程师. 研究方向为嵌入式系统研究与应用.