一种新的隐蔽通信算法

张华熊,张朝阳,仇佩亮
(浙江大学信息与电子工程系,浙江杭州 310027)

摘 要: 近年来,在通信领域隐蔽通信技术正越来越受到重视.本文提出了一种新的实时隐蔽通信算法,该算法利用了混沌序列具有容易生成、对初始条件敏感,以及具有白噪声的统计特性等特点,有效地解决了隐蔽通信技术的两个问题:同步以及突发信息的接收.实验结果表明这种算法是非常有效的.

关键词: 信息隐藏; 隐蔽通信; 同步; 突发信息; 混沌序列
中图分类号: TP391.41 **文献标识码**: A **文章编号**: 0372-2112 (2003) 04-0514-04

A Novel Algorithm of Covert Communication

ZHANG Hua-xiong, ZHANG Zhao-yang, QIU Pei-liang
(Dept. of Information & Electronic Engineering, Zhejiang University, Hangzhou 310027, Zhejiang, China)

Abstract: In recent years, covert communication techniques have become important gradually in communication fields. In this paper, a novel real-time covert communication scheme has been proposed. This method makes use of good properties of chaotic sequences, such as ease of generation, sensitive dependence on their initial condition and noise-like statistic characteristics. Two key problems, synchronization and receiving burst messages, have been solved effectively. Experimental results indicate that these techniques are very effective.

Key words: information hiding; covert communication; synchronization; burst messages, chaotic sequences

1 引言

随着科学技术的发展,人们的隐私以及一些重要的商业及军事信息比以前更容易受到侵犯.因此怎样在传播中保护这些秘密信息已经成为当今通信技术领域的一个重要课题.如果用传统的加密技术,经过加密的信息大多会变得混乱不堪,这样一来容易引起一些别有用心的人的注意.随着数字化技术的发展,信息隐藏技术被深入研究并广泛应用于军事及商业的信息通信中,信息隐藏是一门古老的技术,它通常以音频,视频或图像中的一种作为载体,将秘密信息嵌入到其中,以一种只有接收者才知道信息存在的秘密途径传送信息.和加密技术相比,信息隐藏的目的在于保证隐藏的信息不引起人们的注意,从而减少被侵犯的可能,而加密技术着重于隐藏秘密信息的内容.

典型的信息隐藏算法包括 LSB[1],Patchwork[2]算法,类似于通信中扩频技术的扩频算法[3]等,在这些算法中,信息隐藏的载体大多是音频、视频或图像中的一种,也就是说将秘密信息嵌入到这些载体中进行传输.本文提出了一种实时的隐蔽通信算法,该算法以语音信号作为载体,将一些秘密信息嵌入到其中,从而将这些秘密信息不引人注意地安全传送到接收者.在实际的通信过程中,秘密信息是以突发的形式发送的,也即在接收者收到的音频信号中有可能含有秘密信息,也可能没有.所以实时隐蔽通信算法的一个关键问题就是如何同步,以便信息的正确接收.本文利用混沌序列具有容易生成、对初始条件敏感,以及具有白噪声的统计特性等特点,有效地解决了这个问题.

本文第二部分简单论述了实时隐蔽通信系统模型及其特点.第三部分提出了混沌序列的产生方法.第四部分讨论了为了实现实时通信所采用的快速整数 Haar 小波变换算法.第五部分提出了秘密信息的嵌入和检测算法.最后给出了实验结果及结论.

2 隐蔽通信系统模型

本文提出的隐蔽通信系统模型可以用图 1 来描述.在图 1 中第一个虚线框中是信息发送部分,语音信号 *Speech* 经 A/D 采样(采样频率为 16KHz,16 比特量化),后由高速数字信号处理器(DSP)将秘密信息 M 用文献[4]中提出的抖动量化算法嵌入,语音信号以每帧包含 64 个样本点的形式通过无线或有线信道传送到信息接收方,信息接收方在收到语音信号后由 DSP 用检测算法从中提取出秘密信息 M,同时还将语音信号经 D/A 变换后输出.该隐蔽通信系统应具有以下特点:

(1) 秘密信息是以突发的形式进行发送的,也就是说信道

收稿日期:2001-10-11;修回日期:2002-07-29

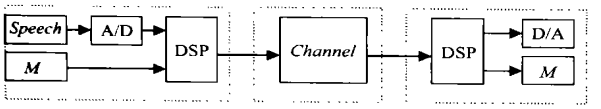

图 1　隐蔽通信系统模型框图

的占用并不是长期或永久性的.

(2) 秘密信息发送方在发送的语音信息中,并不一定要嵌入秘密信息 M,也即秘密信息的嵌入也是随机的或者说是突发的. 信息接收方必须能够对接收到的语音信息作出正确判断,从而从中正确抽取出秘密信息.

(3) 应该具有一定的安全性,最好即使算法被公开也不会对系统造成威胁.

(4) 应该满足实时通信的要求.

3　混沌序列的产生

混沌现象是在非线性动力系统中出现的确定性的、类似随机的过程,这种过程既非周期又不收敛,并且对初始值有极其敏感的依赖性. 一个一维离散时间非线性动力系统定义如下:

$$X_{k+1} = f(X_k) \tag{1}$$

其中, $X_k \in V$, $k = 0,1,2,\cdots\cdots$,称其为状态;而 $f: V \to V$ 是一个映射,将当前状态 X_k 映射到下一个状态 X_{k+1},如果从初始值 X_0 开始,反复应用 f,就得到一个序列 $\{X_k \in V, k = 0,1,2,\cdots\cdots\}$,这一序列称为该离散时间动力系统的一条轨迹.

一类非常简单却被广泛研究的动力系统是 Logistic 映射,其定义如下:

$$X_{k+1} = 1 - \lambda X_k^2 \qquad \lambda \in [0,2] \tag{2}$$

文献[5]中指出在上式中如果取 $\lambda = 2$,则理论上无论取何初值,产生的序列都将是混沌的. 但实际上该公式在某些初值点上经过很短的几次迭代后,它们或者迅速收敛到一稳定点,或者进入周期循环. 为此我们采用文献[5]中提出的用 m 序列(即最大长度线性反馈移位寄存器序列)加扰的方法加以改进,具体的计算公式为:

$$\begin{cases} x_{n+1} = 1 - 2x_n^2 & \text{if } m\_sequen = 1 \\ x_{n+1} = 1 - 2(x_n + D)^2 & \text{if } m\_sequen = 0 \end{cases} \tag{3}$$

上式中 m_sequen 代表 m 序列值, X_n 是加扰后产生的混沌序列,扰动幅度 $D = 0.01$. 在加扰的过程中应注意限制加扰后的值在 $(-1,1)$ 之间.

这样利用上面改进的算法设定迭代的初始值 X_0,就可以得到一个半无限长的实数值序列,从该实数值序列的第 P 个位置开始抽取 L 个元素组成一个长度为 L 的混沌序列,然后将该序列以以下公式映射为由 $-1,1$ 组成的序列,同时将三个参数 X_0, P, L 作为信息检测时的密码保存.

$$W_i = \begin{cases} 1 & \text{if } x_i \geq 0 \\ 0 & \text{if } x_i < 0 \end{cases} \tag{4}$$

在实际应用中,为了防止混沌序列由于计算机有限精度的问题而出现收敛或周期循环,对选取的混沌序列最后要进行周期性和是否收敛进行检查,如果出现收敛或周期循环程序会提醒用户该初值 X_0 不可用,请求重新设定.

4　整数小波的快速算法

小波变换理论是近年来兴起的一种时(空)频域分析理论,在图像和音频信号的压缩编码中得到了大量的应用. 本文利用文献[6]中提出的快速整数可逆 Haar 小波变换对音频信号进行分解,在计算过程中不产生任何浮点运算,既可以精确重构又可以快速实现,从而能够利用 DSP 进行实时隐蔽通信的实现. 文献[6]中提出的快速整数可逆 Haar 小波分解可以用图 2 所示的二叉树结构图来表示:其中 C_{ij} 表示一个低频系数, i 表示分解层号, j 表示该分解层号内的第 i 个低频系数. 第 0 层表示最精细层(相当于原始信号),层号越大,分辨率越低,此时的系数反映的是原始信号的低频特征.

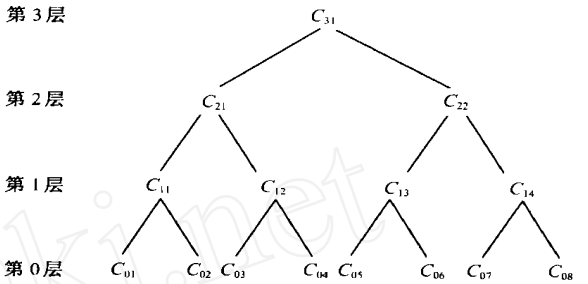

图 2　快速整数可逆 Haar 小波分解的二叉树结构

从图 2 可以看出,第一层的低频系数 C_{11} 可以由第 0 层的两个低频系数 C_{01} 和 C_{02} 来计算得到,该计算过程包括一次加法,一次减法,一次除 2,一次舍入变成整数共四次操作. 其中除 2 和舍入可以简化成一次移位操作. 也就是说在小波分解的过程中,一个低频系数可以通过对上一层两个低频系数的三次操作得到,而这三种操作是 DSP 中最简单的三种基本操作. 如果要求第三层的一个低频系数,只要选取相应的 8 个第 0 层的系数经过 21 次基本操作就可得到. 所以其计算速度是非常快的,完全能够满足实时计算的要求.

5　秘密信息嵌入和检测算法

在秘密信息的嵌入算法中,语音信号被分割成长度为 1024 个样本的段,嵌入是按段进行的. 由于每段的嵌入和检测算法都相同,所以在本文算法的描述中,为简单起见,我们认为都是对语音段操作. 在此定义数字语音信号段用 S 表示,秘密信息用 M 表示,由式(3) 和(4)产生的混沌序列用 W 表示,长度为 128 个比特. 在本文的隐蔽通信系统中,将 ASCII 码 0 到 255 用 256 组采用不同的密码 K(包含三个参数 X_0, P, L) 产生的混沌序列表示,这 256 组混沌序列就相当于通信编码中所说的码书. 这 256 个密码 K 通信双方可以事先约定或通过其他安全的途径得到. W_u 表示从不知是否嵌有秘密信息的语音信号段中抽取的比特序列.

5.1　秘密信息嵌入算法

Step1:设立一个数据缓冲区,每次通信时,当经 A/D 采样得到的样本点达到 1024 时,对该段语音信号作 4 层整数 Haar 小波变换.

Step2:将要发送的秘密信息 M 拆成一个个的字节,根据每个字节的值从码书中选取对应的混沌序列,然后利用文献[4]中提出的抖动量化数字水印嵌入算法,将这个长度为 128 比特的混沌序列嵌入到 Haar 小波变换的 128 个中频系数中. 抖动量化强度取为 1024 或 2048,它们均为 2 的整数次幂,这主要是为了能够利用移位操作来代替除法操作,从而减少计算量,以便满足实时通信的需要. 为增强秘密信息的安全性,在抖动量化后可加一个小的随机噪声来起到随机化的作用,但由此也会相应地造成系统的鲁棒性下降.

Step3:将上面处理后的小波系数进行整数 Haar 小波反变换,从而得到嵌有秘密信息的语音信号段,如果在这段语音信号段 S 中不嵌入秘密信息,则不做任何操作,直接将其发送出去即可.

5.2 秘密信息检测算法

Step1:利用 256 个密码 K 产生抽取秘密信息所需要的码书.

Step2:当接收到的语音信号样本点达到 1024 个时,对该语音信号段进行四层快速整数 Haar 小波变换,并从中提取出 128 个中频系数,利用文献[4]中提出的抖动量化数字水印检测算法抽取出长度为 128 个比特的序列,将这个比特序列分别与码书中的 256 个混沌序列做相关运算.

$$Coff(k) = \sum_{i=1}^{L} W_u(i)\, W_k(i) \tag{5}$$

在上式中,$Coff(K)$ 表示从接收到的语音信号段中抽取出的可疑比特序列与码书中第 $K(K=1...256)$ 个混沌序列的相关值,这样每次能够得到 256 个相关值. 如果接收到的语音信号段中没有嵌入秘密信息,则抽取出的可疑比特序列具有白噪声信号的特点,所以 256 个相关值都应该是一个较小的值(理论上为 0). 如果该段语音信号中嵌有秘密信息,则 256 个相关值中理论上讲应该有一个峰值. 由此我们的解码规则为:首先从 256 个相关值中找出一个最大的相关值 $Coff(\max)$,然后求剩下的 255 个相关值的标准差,将该标准差的三倍作为判决门限 T 的值. 然后将 $Coff(\max)$ 与 T 比较来判决某段语音信号是否带有秘密信息. 如果它大于 T,则该段语音信号中含有秘密信息,并且根据判决得到的混沌序列可以从码书中查出对应的 ASCII 字符值. 如果它小于 T,则表示该语音信号段不带有秘密信息. 由概率论中的中心极限定理知道当分段长度 L 足够大时,$Coff(\max)$ 近似符合高斯分布,则由概率论的知识可知对某段语音信号来说,将不含秘密信息而误报为有秘密信息的概率为 0.0026. 在实际的系统中我们将标准差的五倍作为 T 的值.

5.3 系统同步问题

在本文的第二部分提到系统进行信息的传送是突发的,因此系统的同步是必要的. 在系统开始通信以前,将一个特定的 8 字节长的字符串作为同步码经编码成混沌序列发送出去,接收方在收到该同步码后表示同步成功,可以进行接收和解码. 另外如果发送方在较长的一段时间内只发送语音载体,而没有秘密信息嵌入其中发送,我们规定发送方在发送秘密信息以前必须先发送同步码,以便接收方重新进行同步.

5.4 秘密信息的隐蔽性问题

秘密信息嵌入到语音载体中,应保证该语音信号不会产生较大的失真,也即秘密信息有较好的不可觉察性. 本系统主要通过两方面来达到此要求,一是将秘密信息嵌入到语音载体的中频部分,从而在秘密信息的鲁棒性和不可觉察性之间找到一种妥协. 另外,采取在语音能量的快速上升点开始嵌入秘密信息,从该点开始认为此后的 1024 个样本点是语音信号,有较大的能量可以嵌入秘密信息. 如果不是快速上升点,则可认为此时相当于语音之间的间歇期,此时能量很小,不适合于嵌入秘密信息. 快速上升点的判断是通过该语音信号第四层 Haar 小波变换系数的第一和第二个低频系数之间的差来确定,当两者差值大于某一门限时就认为是快速上升点从而允许该语音段进行秘密信息嵌入.

6 具体实验结果

由于系统的实时性可以通过降低嵌入容量来达到,所以以下的实验主要集中于系统的安全性,秘密信息的嵌入容量及抗压缩的能力. 首先选取了一段采样率为 22.05kHz,16 比特量化,长度为 10 秒的语音信号(其中既有男声也有女声)作为秘密信息的载体.

(1) 安全性实验. 将一个由密码($X_0 = 0.3$, $P = 10000$, $L = 128$)产生的混沌序列嵌入到一段长度为 1024 的语音载体中. 图 3 是利用 800 个不同序列进行检测的结果,图中 x 轴为 800 个不同序列,它们的长度都为 128 比特,初始值 X_0 从 0.001 到 0.8,每次增加 0.001,y 轴为 800 个不同序列所对应的检测结果,图中进行了归一化处理. 从图中可以看出,其中第 300 次对应初始值 $X_0 = 0.3$ 的序列得到了显著的检测结果,由此可知,在不知道系统密码的前提下,要想检测出载体中是否嵌有秘密信息是相当困难的.

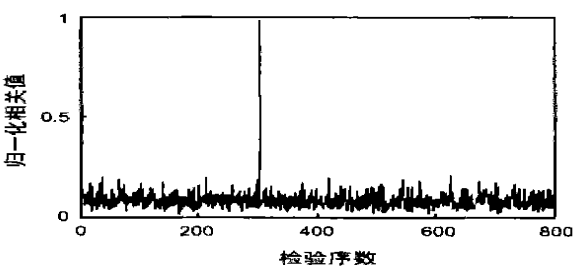

图 3 嵌有一个混沌序列的检测结果

(2) 嵌入容量实验. 由前述可知,系统嵌入容量并不固定,它是随不同的语音信号以及语音信号载体快速上升点检测门限的不同而随时变化的,比如在实时的语音通信中,如果双方均不讲话或讲话声很小,此时由于系统无法检测到快速上升点,从而无法嵌入秘密信息,此时系统的嵌入容量可以说几乎为 0. 而最大可嵌入容量,对于采样率为 22.05kHz,16 比特量化的 1 秒语音信号载体理论上讲为 21 个字节(168 个比特),我们选取的 10 秒语音段实际嵌入容量为 171 个字节(嵌入时的抖动量化值取 1024,快速上升点门限为 100,语音分段长度为 1024),这是由于该语音段是两个人的对话,其中只有很少的语音停顿,所以嵌入容量较大.

(3)抗噪声实验. 我们将上面嵌有 171 个字节秘密信息的 10 秒语音信号段加不同强度的白高斯噪声,从而得到不同信噪比下能够正确恢复的秘密信息的百分比(见表 1). 从表中可以看出,在信噪比 17dB 以上有较高的正确解码百分比,而当小于 15dB 时,则性能急剧下降.

表 1　不同信噪比下秘密信息正确解码百分比率

信噪比(dB)	40	35	30	25	20	17	15
正确解码比率(%)	100	100	96	94	94	89	55

(4)抗压缩实验. 对该段嵌有秘密信息的语音信号分别用 IMA-ADPCM,GSM6.10,MP3 三种压缩算法进行压缩,然后再解压后进行秘密信息的提取. 表 2 为正确解码百分比数据. 从表 2 看出,当抖动量化值取 1024 时该算法在高压缩比(1:10)的情况下性能较差. 当抖动量化值取 2048 时,性能有很大的提升,但此时语音的质量也相应降低,能听出有噪音存在.

表 2 不同压缩算法下秘密信息正确解码百分比率
(抖动量化值取 1024 或 2048)

压缩方法	MP3	GSM6.10	IMA-ADPCM
压缩比	(1:10)	(1:10)	(1:4)
正确解码比率(抖动量化值取 1024)	73 %	62 %	93 %
正确解码比率(抖动量化值取 2048)	92 %	83 %	100 %

7　结论

本文提出了一种实时隐蔽通信系统模型,并利用混沌序列具有容易生成、对初始条件敏感,以及具有白噪声的统计特性等特点,有效地解决了同步和秘密信息突发接收的问题. 但是在具体的通信系统中,为了进行低码率的信息传送,都要对传送的信息进行压缩,并且压缩方法各式各样,而本文的算法在高压缩比的情况下误码率较高,因此研究一种能够在极低码率的信息载体中高可靠地传送秘密信息的隐蔽通信技术将是我们今后所要解决的一个重要问题.

参考文献:

[1] Jong Won Seok, Jin Woo Hong. Audio watermarking for copyright protection of digital audio data[J]. Electronics Letters, 2001, 37(1): 60-61.

[2] Ikeda, M Takeda, K Itakura, F. Audio data hiding by use of band-limited random sequences[A]. IEEE International Conference on Acoustics, Speech, and Signal Processing[C]. Arizona, USA: 1999: 2315-2318.

[3] Ye Wang. A new watermarking method of digital audio content for copyright protection[A]. Proceedings of the Fourth International Conference on Signal Processing[C]. Beijing, 1998: 1420-1423.

[4] M Ramkumar, A N Akansu, Self-Noise suppression schemes for blind image steganography[A]. SPIE's International Symposium on Voice, Video and Data Communications, Multimedia Systems and Applications[C]. Boston, USA. Vol. 3845, 1999: 55-66.

[5] 赵艳红,吴楚,张春. 性能优良的数字混沌序列发生器研究[A]. 中国电子学会电路与系统学会第十六届年会论文集[C]. 宁波,中国电子学会电路与系统学会, 2001, 172-176.

[6] 田金文,柳斌,柳健. 用整数 Haar 小波变换和分块 DPCM 实现静止图像数据的信息熵保持型压缩编码[J]. 通信学报, 2000, 21(11): 29-34.

作者简介:

张华熊　男,1971 年生于浙江省义乌市,现为浙江大学信息与电子工程系博士研究生,主要研究方向为信号处理,隐蔽通信,数字水印技术,本文的研究受到浙江省综合信息网技术重点实验室支持. E-mail: zhxhz@netease.com

张朝阳　男,1973 年生于湖北黄岗,博士,副教授,IEEE Member,1994 年 7 月毕业于浙江大学信息与电子工程学系,获无线电技术专业学士学位。同年被保送攻读通信与电子系统专业博士学位,1998 年 10 月博士毕业后留校任教,主要研究方向为无线移动通信,宽带接入系统,数字电视广播传输系统.

仇配亮　男,1944 年生于上海,现为浙江大学信息与电子工程学系教授,博士生导师,主要研究方向为信息论与编码,通信信号处理、信息安全、低功耗通信技术等.