一种混沌加密算法的硬件实现

陈 滨，刘光祜，张 勇，周正欧

(电子科技大学电子工程学院 成都 6100054)

【摘要】在现有的二相混沌加密算法研究的基础上，提出了一种改进的实用混沌加密算法，使其有限字长效应得到了改善，并借助于数字信号处理器TMS320VC5402实现了改进方法。硬件实验结果表明，该方法具有一定的实践可行性和直接的实际应用意义。

关 键 词 实时； 混沌加密； 二相混沌编码； 伪随机码
中图分类号 TN975；O332 文献标识码 A

A Hardware-Realized Method of Chaotic Encryption

CHEN Bin，LIU Guang-hu，ZHANG Yong，ZHOU Zheng-ou
(School of Electronic Engineering, UEST of China Chengdu 610054)

Abstract On the basis of 2-phase chaotic coding, a novel useful chaotic encryption method is proposed and is realized on the digital signal processor – TMS320VC5402. The hardware result shows that the effect of limited word length is improved.

Key words real-time; chaotic encryption; 2- phase chaotic coding; pseudo noise code

随着第三代移动通信系统的蓬勃发展，保密通信变得日益重要。在这方面，传统的伪随机(Pseudo Noise，PN)码加密方案显得不能满足要求，主要体现在PN码的数量有限上。混沌的固有特性决定了它可以被用于保密通信。混沌映射对初值的极端敏感性，即所谓的“蝴蝶效应”，使得它对于不同的初值，可以产生大量确定的、不相关的、类似随机的序列簇。文献[1]提出了一种实用的混沌加密通信系统，文献[2-4]分析了二相混沌序列的统计特性及其用于扩频或跳频通信的情况，并通过数值实验将它们的性能与PN码做了对比。对于二相混沌序列的理论研究近于达到成熟，而对于实际应用，还需要对有限字长效应等作进一步的研究。本文对文献[1]提出的方法进行了改进，并借助硬件电路实现了改进的方法。

1 混沌加密算法

混沌加密解密的过程如图1所示，与传统的PN码加密解密过程相同，最关键的部分是加密解密的混沌序列构造。图1中的调制、解调可用模2和或异或算法来实现。这里使用单峰的logistic映射，其表达式为：

$$x_{k+1} = ux_k(1-x_k)\text{，}\quad x_k \in [0,1]\text{，}\quad u \in [0,4] \tag{1}$$

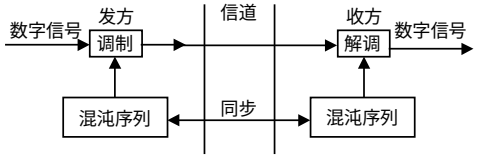


图1 混沌加密解密过程

文献[2-4]关于式(1)用于加密的性能在理论上做了大量的分析，在实际应用中更注重字长对产生混沌序列的影响。对于16 bit定点的TMS320VC5402，根据混沌的遍历性，随着时间的推移，混沌序列必将演化为一个周期序列，而最长的叠代次数必然低于2^{16}，实际情况下，可能的叠代次数会更少一些。为了增加字长

收稿日期：2003 –12 – 24
作者简介：陈 滨(1971 –)，男，博士生，主要从事混沌保密通信方面的研究.

效应造成的周期，文献[1]采用多级级联的方法。例如对于二级级联情况，文献[1]强调一个混沌映射定时为另一个混沌映射产生初值序列，两个混沌映射之间没有相互耦合。于是，本文提出了相互耦合的改进，即一个混沌映射定时为另一个混沌映射提供初值的同时，另一个混沌映射也定时为前一个混沌映射提供初值。同时，对文献[1]所表述的实值序列，按峰值点进行二值化，即作如下约定：

$$c_k=\begin{cases}1, & x_k \geq 0.5\\ 0, & x_k < 0.5\end{cases} \quad \text{或} \quad c_k=\begin{cases}1, & x_k > 0.5\\ 0, & x_k \leq 0.5\end{cases} \tag{2}$$

式中　$\{c_k\}_{k=0}^{N-1}$ 即为混沌序列。对于二级级联情况产生混沌序列的方法如图2所示。

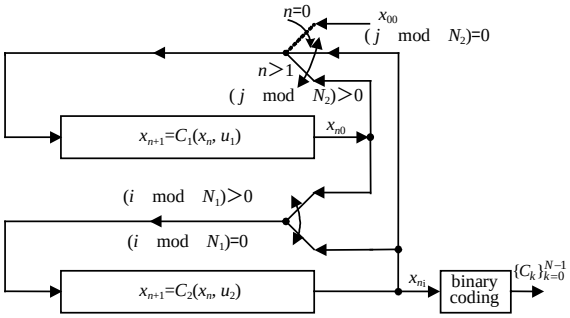


图2　改进的混沌序列产生方法

图2中，$x_{n+1}=C_1(x_n,u_1)$ 和 $x_{n+1}=C_2(x_n,u_2)$ 为两个映射，这两个映射可以相同，也可以不同，u_1 和 u_2 控制参量，对于相同的映射应取不同值。i 和 j 为计数变量，一般可令 $N_2 >> N_1$，初始状态 $n=0$ 时，将初值 x_{00} 赋给映射 C_1、C_2 每叠代 N_1 次就通过 C_1 改变一次初始值，同时，C_1 每叠代 N_2 次就通过 C_2 改变一次初始值。C_1 是慢叠代，C_2 是快叠代，C_2 每作 N_1 次叠代 C_1 叠代一次。可以作适当次数的预叠代，以跳过映射的渐变区。采用图2的双向耦合的方法可以保证经过相当长的时间后，即使有一个映射产生的混沌序列演化为周期序列，也因它与另一个映射交换初值而跳出周期态，以有效地克服实际系统中产生混沌序列的周期化效应。数据仿真分析表明：文献[1]的方法周期长度约为3 800步，改进的方法在几乎不增加运算量的基础上，周期长度增加到约为7 200步。

在实际系统中，由图2的 $\{c_k\}_{k=0}^{N-1}$ 产生用于加密和解密的混沌序列的方法是这样的：构造一个长为L的空队列，这个队列称为框架队列。第一次参与运算时，必须由 $\{c_k\}_{k=0}^{N-1}$ 充满整个框架队列。其后，每叠代一次固定地由框架队列一端进入一个 c_k，而另一端则有一个二值码出队，框架队列的长度不变。更新框架队架的方法也可以有多种，一般使用顺序更新即可，也可以使用部分随机洗牌的方法。当L=1时，即为简单的混沌加密；当L>1时，即为混沌扩频加密，这里通称为混沌扩频加密。

从图2中还可以看出，收发双方只需要约定初值和两个映射的形式(公钥和密钥可以灵活选择)，实际通信时将工作时钟定时器同步了，即可以达到收发双方加密和解密的同步。

2　MATLAB仿真

结合实际的加密和解密运算，就上述算法设计出的有限字长混沌序列，使用MATLAB作数值分析。对于框架队列的长度L较短的情况，例如L<10时，考虑其相关和平衡性能没有太大意义，这时就视为普通的加密；当框架队列较长时，则有必要分析一下混沌序列的相关和平衡性，这时视为混沌扩频加密。对于L=1的加密，在解密时只要对应地产生一位解密位参与异或即可；对于L>1的情况，在解密时不但要产生对应位的解密序列参与异或运算，而且，还要对结果位进行求和，并设置判决门限为0.809 6，根据求和结果和门限比较大小来判定信息位。

给定序列 $\{a_n\}_{n=0}^{L-1}$ 和 $\{b_n\}_{n=0}^{L-1}$，取值为{0，1}，定义它们的归一化“相关”函数(或称为相似性)为：

$$SIM(m)=\frac{1}{L}\left(\sum_{i=0}^{L-1} a_i \otimes b_{(m+i) \bmod L}\right) \tag{3}$$

式中　“$\otimes$”为同或运算。如果两个序列完全不相同，则式(3)的结果为0，如果两个序列完全相同，则式(3)

的结果为1。显然，相似性的中值点0.5对应于相关性的0点。由式(3)引申出下面两个峰值参量为衡量标准，即序列最大自相似(旁瓣)：

$$SS = \max_{m>0} SIM_{aa}(m) \tag{4}$$

序列最大互相似：

$$CS = \max_{m} SIM_{ab}(m) \tag{5}$$

显然，对于无噪声解密的情况，式(3)的结果为1。序列最大自相似(旁瓣)和序列最大互相似，即式(4)和(5)计算的结果与1有明显偏离是所期望的。于是，把区间[0.5,1]黄金分割，即把实际有噪声影响情况下，只要式(3)的结果在0.809以上，即认定为正确解密。在MATLAB数值分析时，认定公式(4)和(5)这两个指标均小于0.809，则可以保证不考虑噪声情况下的正确解密，当然以上两个指标越接近0.5越好。如果选取了 D 组序列参与运算，其中的 $D-1$ 组序列设定为干扰序列，计算后 SS 和 CS 大于0.809的序列个数记为 E，则定义解密出错的概率为 $P_e = E/D \times 100\%$，随着序列的演化定义一个随序列演化而解密出错的概率，不妨设定为各次演化的最坏情况，即定义 $P_{em} = \max P_e$。

选取了100个不同的初值(将区间(0.3,0.4)进行100等分划分)，动态产生100组混沌序列参与运算(跳出渐变态的步数 C_1 设为20步、C_2 设为L+20步)，即 $D=100$，设定 $u_1 = 3.92$ (u_1 是密钥，应设置为不规则数值)，$u_2 = 4.0$，框架队列的长度 L 从10到1 000不等，$N_1 = 2L$，$N_2 = 10L$，演化步数为1 000步，数值分析结果如表1所示。

表**1** 混沌序列的相似性分析

指标	框架队列长序							
	10	20	40	80	100	200	500	1 000
SS	1.000	0.800	0.800	0.700	0.720	0.650	0.612	0.606
CS	1.000	1.000	0.875	0.788	0.780	0.710	0.648	0.622
P_e	1.000	0.914	0.127	0.000	0.000	0.000	0.000	0.000

表1中给出的是序列演化过程中最坏的情况，从下面的分析可以看出表1所得的结果具有代表性和一般性。(1) 当序列较短时，例如<40时，序列可以作为加密序列，做为扩频序列则效果较差，即抗多址和多径能力不是很好；(2) 当序列逐渐加长时，序列的相似性变差，相关性能变好，即使因噪声改变了序列中位的极性，在黄金分割下不会影响数字解扩的正确性；(3) 因为考虑了最坏情况的解密出错概率，实际应用中一般不可能达到，所以对于扩频加密来说，序列长度达到40以上就可以了。

同时，当将初始值作为密钥处理时，控制参量 u_1 和 u_2 可以相同。当初始值作为明钥时，控制参量应不相同，且 u_1 尽可能为不规则数，因为，这时映射 C_1 起到了一个明钥生成密钥的作用。

3 硬件实验

硬件实验所完成的功能如图3所示。

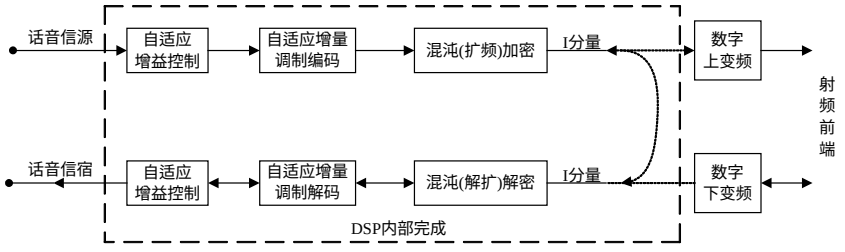
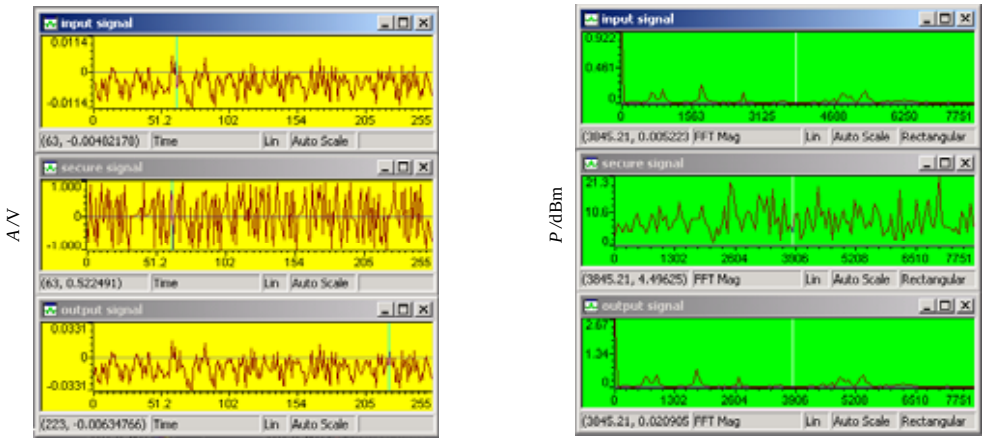


图3 算法实现的功能

由麦克风或音频输出设备作为输入信号源向SY5402EVM板送入话音信号，在SY5402EVM板上经过TLC274放大器放大后，送给TLC320AD50编码器做模数转换，得到的话音数字信号经EPM7128SLC84缓冲后，输入TMS320VC5402完成信号的自适应增益控制(Adaptive Gain Control，AGC)[5]、自适应增量调制(Adaptive Delta Modulation，ADM)编码和混沌(扩频)加密后，若是实际通信系统中应该送出到外部数字上变频器或数模转换器。这里重点是完成混沌加密算法，所以，在TMS320VC5402内部作了一个小循环，如图3所示。即完成混沌加密后的信号又在其内部完成混沌解密、ADM解码和AGC，经过缓冲 、数模变换 、放大之后，输出还原的话音信号。

使用CCStudio实时捕捉了输入话音信号和输出话音信号的波形。图4设置了3个长度为256的存储区段，给出了直接对AGC后的某时刻信号(没有做ADM处理)进行加密前、加密后和解密后的信号波形和谱，从图4上可以看出混沌加密具有扩展频谱的作用。



a. 时域波形　　b. 频域频谱

图4　加密信号与加密前后的信号波形和频谱幅度对比

4　结 束 语

本文基于文献[1]的混沌加密方法提出了一种改进的混沌加密方法，并通过MATLAB数值仿真和硬件实验实现了改进方法，分析及试验结果表明改进方法具有运算量小、加密性能好等优点，从而具有一定的实际应用价值。

参 考 文 献

[1]Heidari-Bateni G. A chaotic direct-sequence spread-spectrum communication system[J]. IEEE Trans. on Communications, 1994, 42: 1 524-1 527.
[2] 王　亥, 胡健栋. Logistic-Map混沌扩频序列[J]. 电子学报, 1997, 25(1): 19-23.
[3] 凌　聪, 孙松庚. Logistic映射跳频序列[J]. 电子学报, 1997, 25(10): 79-81.
[4] 蔡国权, 宋国文, 于大鹏. Logistic映射混沌扩频序列的性能分析[J]. 通信学报, 2000, 21(1): 60-63.
[5] 张　勇. C/C++语言硬件程序设计-基于TMS320C5000系列DSP [M]. 西安：西安电子科技大学出版社, 2003.

编　辑　孙晓丹