第 57 卷 第 3 期 2008 年 3 月
1000-3290/2008/57(03)/1409-07

物 理 学 报
ACTA PHYSICA SINICA

Vol.57,No.3,March,2008

一种混沌扩频序列的产生方法及其优选算法*

余振标 冯久超†

(华南理工大学电子与信息学院,广州 510641)

(2007 年 4 月 23 日收到;2007 年 6 月 4 日收到修改稿)

提出一种基于组合映射模型产生混沌扩频序列的方法. 根据扩频序列的特性要求和多址干扰性能指标,给出了一种混沌扩频序列的优选算法;将得到的优选序列应用于直扩码分多址系统,在不同信道条件下进行仿真,并与优选的 Logistic 混沌扩频序列进行性能比较,结果表明本方法产生的混沌扩频序列具有和 Logistic 混沌扩频序列相近的良好性能,而且保密性更好.

关键词:码分多址,优选算法,多径信道,误码率

PACC:0545

1. 引 言

直扩码分多址(DS-CDMA)系统的主要干扰是同时接入的多个用户带来的多址干扰(MAI),因此要求使用的扩频序列具有良好的相关性[1]. 混沌信号具有类噪声、伪随机、非周期和对初值极其敏感等特性,根据混沌映射方程,可以产生大量相关性很好的混沌序列[2]. 因此,它非常适合用在扩频码分多址通信系统中.

目前已有的混沌扩频序列产生方法主要采用一维的混沌映射,该方法简单且易实现. 由一维映射迭代产生的混沌扩频序列[3,4]虽然有比较理想的平衡性和相关性,但是复杂度不高,保密性不理想. 本文提出一种基于组合映射模型产生混沌扩频序列的方法,并将产生的混沌扩频序列与由 Logistic 映射迭代产生的混沌扩频序列的统计特性进行比较分析,仿真结果表明本文方法产生的混沌序列不仅有理想的平衡性和相关性,而且提高了保密性. 本文还提出一种混沌扩频序列的优选算法. 最后将优选的混沌扩频序列应用于直扩码分多址通信系统中并仿真,结果表明本文方法产生的混沌扩频序列适合扩频通信.

2. 混沌序列的产生

2.1. 混沌映射模型

混沌序列由非线性的混沌映射迭代产生. 文献[2—4]指出一维混沌映射产生的混沌序列有比较理想的平衡性和相关性,适合用作扩频序列;但是从保密性角度看,由于一维映射迭代产生的混沌序列容易用预测或反向迭代重构等技术识别[5],保密性不好;因此在实际应用中应合理使混沌映射复杂化,以增强产生的混沌序列的保密性. 本文混沌序列的产生方法是混沌序列不是由一个混沌映射产生,而是由多个不同映射的组合产生. 改进型 Logistic 映射、Chebyshev 映射的取值范围都是(-1,1)[3,4];本文选取这两个混沌映射来构建组合混沌映射,其数学模型如下:

$$x_{n+1} = a_1 + a_2\cos(k_1\cos^{-1}x_n) + a_3x_n^2 + a_4(\cos(k_2\cos^{-1}x_n))^2. \quad (1)$$

选择不同的 a_i 及 k_i,上式对应不同的混沌映射. 当 $a_1=1, a_3=-2, a_2=a_4=0$ 时,为改进型 Logistic 映射;当 $a_1=a_3=a_4=0, a_3=1, k_1=4$ 时,为 Chebyshev 映射;而当 $a_2=a_3=0, a_1=1, a_4=$

* 国家自然科学基金(批准号:60572025),教育部新世纪优秀人才基金(批准号:NCET-04-0813),教育部重点项目(批准号:105137)和广东省自然科学基金(批准号:07006496,04205783)资助的课题.

† 通信作者,E-mail:fengjc@scut.edu.cn

-2，$k_2=4$ 时，就变成了将 4 阶 Chebyshev 映射嵌入到改进型 Logistic 映射中所形成的一个复合混沌映射，它同样具有混沌特征[6]．这个映射实际上是将一个混沌系统嵌入到另一个混沌系统内部，引起原混沌系统的动力学行为的改变，进一步增加新系统的不确定性．Chebyshev 映射和改进型 Logistic 映射的概率分布密度函数[3,4]都是

$$p(x)=\begin{cases}\dfrac{1}{\pi\sqrt{1-x^2}}, & -1<x<1,\\ 0, & \text{其他}.\end{cases} \tag{2}$$

由此可知复合映射方程的概率分布也是关于 0 对称分布的，$x_n\in(-1,1)$，因此在同一种结构下通过参数切换能够实现多种混沌映射．

2.2. 混沌序列产生方案

理想情况下，混沌序列本身是非周期的，但在扩频通信中每个信息比特所含的扩频序列码段的长度是一定的，混沌序列作为扩频序列时就只能截取一段．因此产生序列时，可按照系统最小初始敏感度，选定相当数量的初始值，来产生一定长度的混沌序列．

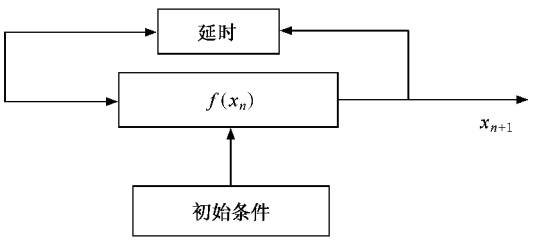

图 1 混沌序列产生方法示意图

本文提出的组合映射模型克服了单一映射可能存在的一些安全隐患，混沌序列产生方法如图 1 所示．在该混沌系统中的初始条件不是一般意义上的简单的映射迭代初始值 x_0，而是包括 x_0、(1)式中的参数 a_i，k_i 以及各个映射的切换规则．这些信息将作为密钥，生成的混沌序列将直接由该密钥决定．

混沌映射迭代产生的序列为实值序列，这种序列本身可以直接作为扩频序列．但是数字通信中有时需要对实值序列数字化，得到二进制混沌序列．本文提出的组合映射模型中各个映射的均值为 0，因此可以采用符号函数转换得到二进制混沌序列

$$C_n=\operatorname{sgn}(x_n). \tag{3}$$

3. 混沌扩频序列性能分析

3.1. 保密性分析

由于可以利用非线性逆推方法估计某些单一的混沌映射的初始值，也可利用混沌序列的统计特性估计某些混沌映射的参数[5]，加上混沌序列实现时的有限精度，单一映射混沌序列存在安全隐患．本文提出的组合映射模型有效地克服一维映射的这一不足．根据(1)式产生混沌序列需要切换其参数，也就是通过在各个混沌映射间切换来提高保密性[7]．参数的切换原则可根据需要任意确定，可以采用等序列间隔，也可以用不等序列间隔，甚至使用随机序列间隔．组合映射混沌序列在不同的时段由不同的混沌映射迭代产生，不同时段的序列对应不同的混沌吸引子．

在通信中，窃听者要对直扩调制的信息进行解密，必须掌握扩频序列的生成结构和变化规律．扩频序列的产生依赖的参数越多，系统的保密性就越好[8]．组合映射要比单一映射复杂得多，迫使窃听者在解密过程中必须分析多个参数及其切换信息．而且在这些参数中 k_i 的变化范围很大，可取大于 2 的整数，即对应于不同阶的 Chebyshev 映射；它们的细微变化都会引起整个序列的巨大改变，很难通过对序列分析找出其映射函数原形．即便窃听者得到了其中的混沌映射函数，但是不知道参数的切换规则，窃听者也几乎不可能重构混沌序列．因此，组合映射混沌序列的最大特点是增强了混沌序列的保密性，适合用于保密通信．

3.2. 平衡性分析

扩频序列的平衡性指二进制序列内“1”与“-1”的码元数目比例，定义为 $E=|M-N|/L$，其中 M，N 分别是“1”与“-1”的个数，L 表示序列的长度．改进型 Logistic 映射、Chehyshev 映射的初始值对其序列的平衡性 E 基本上没有影响，但是有几个特殊初始值会导致平衡性峰值出现，对 Logistic 映射，$x_0=-0.5,0,0.5$；对 Chehyshev 映射，$x_0=0$．原因是这几个初始值是映射迭代的不动点．因此在以本文的组合映射模型产生序列时，初值的选取应避开引起平衡性出现峰值的特殊初值点．文献[9]分析表明 Logistic 映射和 Chebyshev 映射产生的混沌扩频序列

越长，平衡性越好. 下面对在一定参数下组合映射产生序列的平衡性与序列长度的关系进行仿真，并与 Logistic 映射序列进行对比. 仿真结果如图 2 所示，它们是由随机取 10 个不同的初始值产生的序列，运算 10 次取平均得到 E，而各个长度不同的序列是由同一初始值产生. 可以看出，组合映射与 Logistic 映射一样，序列长度增加时平衡性越好，且二者的平衡性相当.

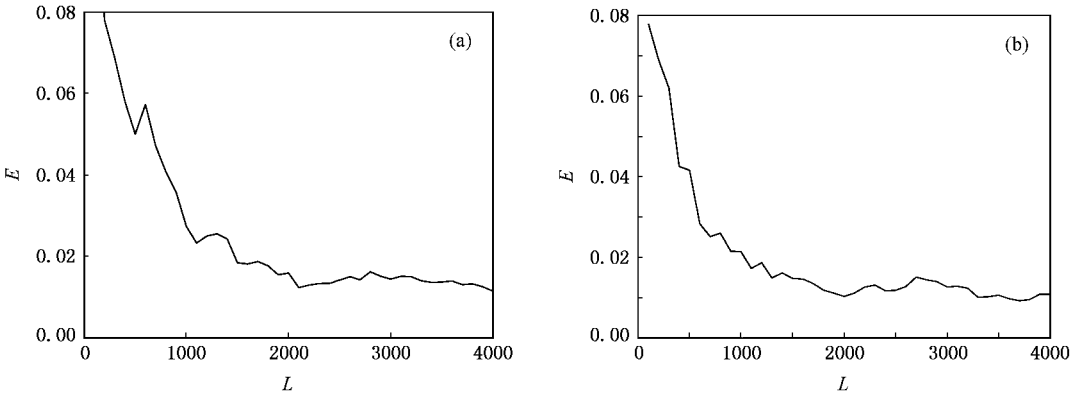

图 2　不同长度序列的平衡性　(a) Logistic 映射；(b) 组合映射

3.3. 相关性分析

1) 自相关函数的定义为

$$R_{ac}(m) = \frac{1}{L}\sum_{k=0}^{L-1} C_k^1 C_{k+m}^1 . \tag{4}$$

2) 互相关函数的定义为

$$R_{cc}(m) = \begin{cases} \dfrac{1}{L}\displaystyle\sum_{k=0}^{L-1} C_k^1 C_{k+m}^2, & m > 0, \\ \dfrac{1}{L}\displaystyle\sum_{k=0}^{L-1} C_k^1 C_k^2, & m = 0, \\ \dfrac{1}{L}\displaystyle\sum_{k=0}^{L-1} C_{k-m}^1 C_k^2, & m < 0, \end{cases} \tag{5}$$

其中 C_k^1 和 C_k^2 是两个不同的二进制混沌扩频序列，L 是序列长度，m 是相关间隔[3]. 图 3(a) 显示一个初始值为 $x_0 = 0.126$，序列长度 $L = 2000$，各个相关间隔长度为 200 的组合映射序列的自相关函数值，相关间隔的范围是 − 1000 到 1000. 从图 3(a) 中可以看出在相关间隔 $m = 0$ 时的自相关函数值为 0.5，自相关旁瓣接近于零. 类似于 δ 函数，接近高斯白噪声的特性.

图 3(b) 显示两个不同(另一序列的初始值 $x_0 = 0.126001$)序列的互相关函数值. 由图 3(b) 可以看出，互相关值非常小，同样接近于白噪声，而且两个序列的初始值只相差 10^{-6}，经过数次迭代后互相关性就变得很小. 组合映射仍然保持了 Logistic 混沌映射的初始值敏感性，加上该混沌系统序列的产生依赖参数的切换，因此只要这两者之一稍有不同，便能产生不同的混沌序列，这个序列的数目是巨大的.

3) 自相关旁瓣与互相关均方值

在 DS-CDMA 系统中某个用户所受到的多址干

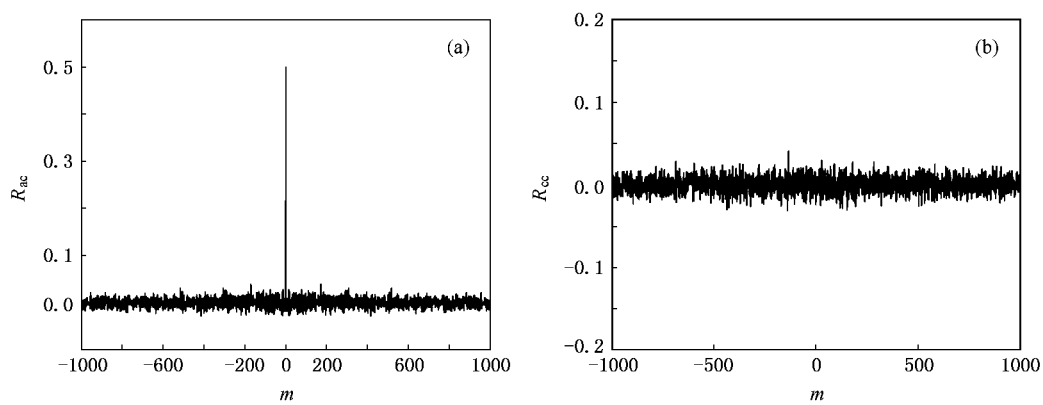

图 3　组合映射混沌序列的相关函数　(a) 自相关；(b) 互相关

扰主要取决于该用户与系统中其他用户的部分互相关函数的平方和. 因此,考虑 DS-CDMA 系统的扩频序列的性能,主要由自相关旁瓣和互相关均方值来表征扩频序列应用于扩频通信系统时抗多径干扰和多址干扰的性能. 混沌二进制扩频序列的这两个性能指标如下[3]:

自相关旁瓣均方值

$$\sigma^2_{R_{ac}}(m) = \frac{1}{M}\sum_{m=0}^{M}[R_{ac}(m)]^2; \qquad (6)$$

互相关均方值

$$\sigma^2_{R_{cc}}(m) = \frac{1}{2M+1}\sum_{m=-M}^{M}[R_{cc}(m)]^2. \qquad (7)$$

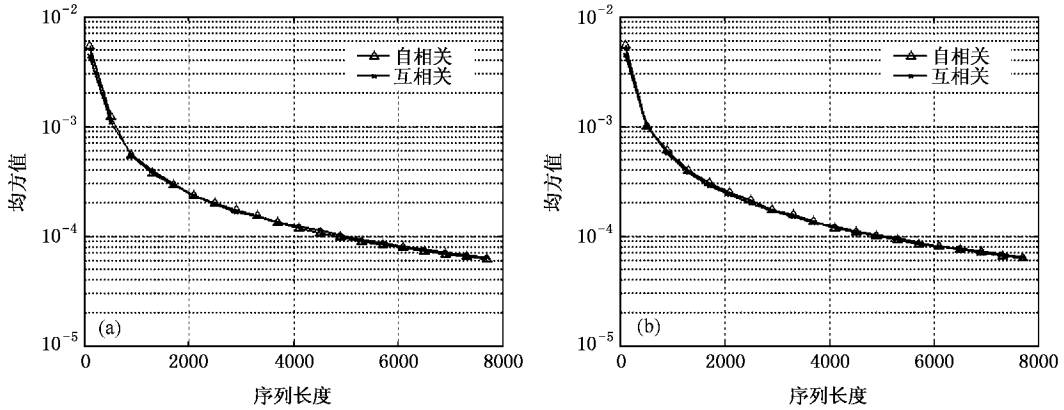

图 4 自相关旁瓣和互相关均方值 (a) Logistic 映射;(b) 组合映射

下面对改进型 Logistic 映射和组合映射产生的扩频序列的性能作比较,由上面定义可以得到两者产生的扩频序列的自相关旁瓣均方值和互相关均方值曲线,如图 4 所示. 改进型 Logistic 映射和组合映射产生的扩频序列自相关旁瓣和互相关均方值的曲线几乎重叠在一起,说明序列长度对自相关旁瓣与互相关均方值的影响几乎一样. 此外,序列越长自相关旁瓣和互相关均方值就越小;但随着序列长度的增加,对这两个均方值的改善也越来越小. 可以看出扩频序列长度在 1000—5000 之间比较合适,因为这个区间的自相关旁瓣和互相关均方值相差不超过 0.001.

4. 扩频序列优选算法

混沌映射可以产生的混沌扩频序列虽然数量众多,但并不是所有的序列都能满足实用要求,必须对其进行优选. 在码分多址通信中,码元数的平衡性与载波抑制度有关,如果不平衡将会使系统的载波泄漏变大,影响系统的性能;因此在进行序列选取时可以用平衡性作为一个优选准则. 文献[10]提出扩频码的平衡性要满足 $E < 0.02$,本文取 $E < 0.01$ 作为优选准则. 文献[11]还指出,扩频序列的自相关旁瓣峰值和平均值表征多径干扰对系统性能的最坏影响和平均影响;而互相关峰值和平均值表征多址干扰对系统性能的最坏影响和平均影响. 在文献[12]中提出采用归一化自相关旁瓣和互相关的最大峰值作为标准来进行优选的方法,其计算量虽较小,但决定 CDMA 系统性能的是相关函数的均方值,峰值仅仅代表了最坏情况[11],不够准确;因此本文把自相关和互相关的峰值和均方值都作为序列优选的准则,这四者分别对应阈值 J_1, J_2, J_3, J_4.

在互相关准则的判定过程中,可将待选序列看作节点,满足互相关准则的两个序列可以认为是互相连通的节点,等价于图论中寻找最大连通集的问题. 目前还没有简便易行的求图的最大连通集的算法. 但是这里的节点图是方阵图,而且各个节点是关于方阵对角线对称的,本文利用这个特点,提出一种简便的寻找最大连通图的算法. 此算法原理如下:设整个集合点的节点数目为 n,定义一个 $n \times n$ 阶方阵 $F_{n\times n}$,方阵的各元素取值如下:当 $i \neq j$ 时,如果满足互相关原则时 $F_{ij} = 0$,否则 $F_{ij} = 1$;当 $i = j$ 时,则设定 $F_{ij} = 0$,即对角线上的元素全部为零. 此时,寻找最大连通图也就是在 $F_{n\times n}$ 中寻找标记为“0”的关于对角线对称的最大维数方阵. 在 Matlab 中实现此算法步骤如下:

第一步,借助 fing(*)函数进行第 1 次判断,此函数用来寻找矩阵中非零元素的下标[13],最大方阵 $F(1:n,1:n)$ 中是否含有“1”,如果函数返回空,则说明 $F(1:n,1:n)$ 不含“1”,就是最大连通图,停止搜

索；否则进入下一步.

第二步，开始第 $i(i=2,\cdots,n)$ 次判断，此时检测方阵为 $T_{m\times m}(m=n-i)$，该方阵沿对角线移动，最多检测次数为 i 次，每移动一次进行一次判断.

第三步，第 $k(k=1,\cdots,i)$ 次移动的检测方阵为 $T(k:k+m,k:k+m)$，若检测方阵不含有“1”，停止搜索，转入第四步；否则，当 $k\leqslant i$ 重复第三步且令 $k=k+1$，当 $k>i$ 且 $i=i+1$ 重复第二步.

第四步，此时 $F(k:k+m,k:k+m)$ 为最大连通图，根据矩阵下标可以找出相应的混沌扩频序列，完成优选过程.

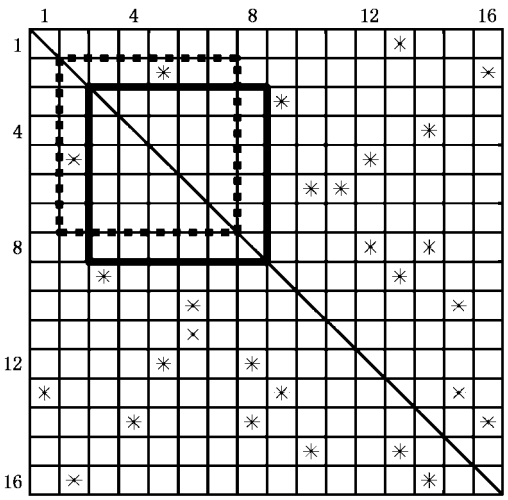

图 5　求最大连通图方法示意图

此方法如图 5 所示，图中打星号的为不满足互相关性的标记；虚线方块中含有星号，不是最大连通图；实线方块中已经没有星号标记，是最大连通图，它是一个大小为 6×6 的方阵. 此算法不必像图像处理中那样对像素进行 4 连通或 8 连通等进行搜索，而是在一定的方块里面直接找出没有符合相关性要求的标记就可以作出判断，即只要 fing(*)一返回空，就停止搜索；虽然此法不是完善算法（互相关连通节点在矩阵位置改变后，此法找到的最大连通图会跟随变化，可根据变化作多次优选，取数目最多的），但其运算量少，不失为简便的办法.

现在对本文提出的组合映射模型产生的混沌扩频序列进行优选. 具体计算方法如下：随机选取 4000 个初始值；为分析方便，混沌序列由等序列间隔参数切换原则，依次由模型中的各映射产生. 各个映射的间隔为 40，用组合混沌映射迭代产生 4000 个序列长度分别为 $L=127,255,511$ 的二进制混沌扩频序列. 然后据设定的阈值对这些序列进行优选.

表 1 给出了 Logistic，Chebyshev 和组合映射产生的混沌扩频序列的优选结果. 其中只给出 J_2 和 J_4 相应选出的序列数目. 由表 1 可以看出，三者所选符合要求的序列数目相当. 随着序列长度的增加，选出的序列越多，而且相关性能越好，与图 5 结果相符. 表 1 说明本文提出的组合映射适合大用户容量扩频系统需要大量扩频序列的要求. 为了便于比较，表 2 列出 Logistic 和组合映射产生的混沌扩频序列自相关和互相关平均值的计算结果. 从表 2 可以看出，优选后得到的两种混沌扩频序列不仅平衡性接近，且自相关和互相关峰值、均值都相当；决定 CDMA 系统性能的是互相关函数均方值[11]，所以两者有相当的系统性能，在下一节仿真验证.

表 1　3 种不同混沌扩频序列的优选序列数

序列长度	J_2	Logistic	Chebyshev	组合映射	J_4	Logistic	Chebyshev	组合映射
127	0.004	264	224	210	0.005	31	31	35
255	0.002	236	216	234	0.003	36	41	43
511	0.001	474	516	472	0.002	148	134	115

表 2　序列长度 $L=255$，优选 Logistic 序列与组合映射序列性能比较

序列	数目	自相关旁瓣峰值平均	自相关旁瓣均方值	互相关峰值平均	互相关均方值
Logistic 映射序列	36	0.1507	0.001795	0.1689	0.001957
组合映射序列	43	0.1449	0.001783	0.1700	0.001967

5. 通信仿真

为了验证本文提出的由组合映射得到的混沌扩频序列与 Logistic 序列同样具有良好性能，将它们应用于直扩码分多址系统，并在 Matlab 环境下进行仿真. 采用 Monte Carlo 方法进行仿真，每一次仿真都在 Logistic 和组合映射混沌优选序列集中随机选取

用户序列,分别对 1 路、2 路和 8 路优选用户序列进行仿真,用户序列长度为 255. 仿真过程中假定序列理想同步.

在只有 AWGN 的情况下,得到的误码率随信噪比变化曲线如图 6 所示,组合映射序列与 Logistic 序列误码率曲线几乎是重合的,可见它们的性能相当,而且与传统扩频多址通信的平均误码率也相当[14].

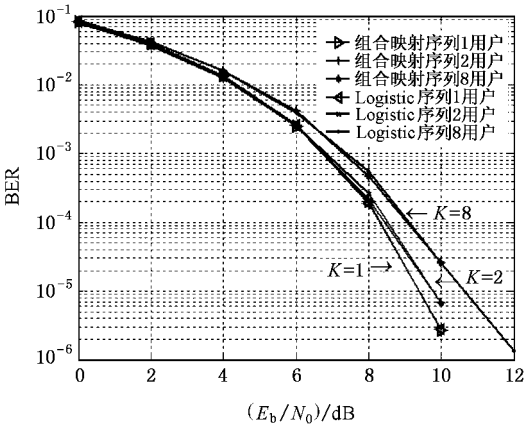

图 6 只有 AWGN 信道中的仿真误码率

进一步考虑多径信道对两种扩频序列性能的影响,现考虑一种多径信道模型,其信道系数矢量是[15]

$$h = [1, 0.45, -0.22]. \quad (8)$$

从图 7 可以看出,多径干扰的存在会使得误码率性能有所下降,但从图中可以看出 Logistic 序列与组合映射序列对应的系统误码性能仍是基本相同,这与表 2 相关性数据相当是一致的.

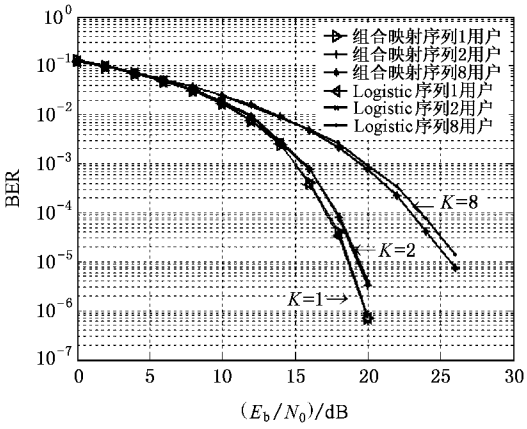

图 7 AWGN 和多径干扰信道中的仿真误码率

6. 结 论

本文用组合映射模型产生混沌扩频序列,比单一映射产生的混沌序列更复杂,增加了预测难度,提高了保密性;此序列不仅有理想的平衡性,而且有良好的相关性. 本文还提出了一种简单的扩频序列优选算法,在对产生的大量混沌序列进行优选时,能有效减少计算量. 最后将产生的混沌扩频序列应用于直扩码分多址系统并仿真,结果表明本文方法产生的扩频序列适合扩频通信.

[1] Sarwate D V, Pursley M B 1980 *Proceedings of the IEEE* **68** 593

[2] Ling C, Li S Q 2000 *IEEE Transactions on Circuits and Systems-I* **47** 394

[3] Wang H, Hu J D 1997 *Journal of China Institute of Communications* **18** 71 (in Chinese) [王 亥、胡键栋 1997 通信学报 **18** 71]

[4] Cai G Q, Song G W, Zhou L L 1999 *Acta Eelectronica Sinica* **27** 74 (in Chinese) [蔡国权、宋国文、周利莉 1999 电子学报 **27** 74]

[5] Ling C 1999 *IEEE Trans. on Signal Processing* **47** 1424

[6] Yu J J, Cao H F, Xu H B *et al* 2006 *Acta Physica Sinica* **55** 29 (in Chinese) [于津江、曹鹤飞、许海波等 2006 物理学报 **55** 29]

[7] Sun L, Jiang D P 2006 *Acta Physica Sinica* **55** 3283 (in Chinese) [孙 琳、姜德平 2006 物理学报 **55** 3283]

[8] Mazzini G, Setti G, Rovatti R 1997 *IEEE Trans on Circuits and Systems-I* **44** 934

[9] Yu S J 2001 *Journal of Shenyang Institute of Technology* **20** 84 (in Chinese) [于舒娟 2001 沈阳工业学院学报 **20** 84]

[10] Lehnert J, Pursley, M 1987 *IEEE Transactions on Communications* **35** 87

[11] Karkkainen K H 1993 *IEICE Trans. Commun.* E**76**-B(**8**) 848

[12] Sandoval-Morantes D, Munoz-Rodriguez D 1998 *Electronic Letters* **34** 235

[13] Zhang Z Y 2003 *Mastering Matlab* 6.5 (Beijing: Beijing University of Aeronautics & Astronautics) (in Chinese) [张志涌 2003 精通 MATLAB6.5 版 (北京 北京航空航天大学出版社)]

[14] Zhu J K 1993 *Spread Spectrum Communication and Its Application* (Beijing: China Science and Technology Press) p44 (in Chinese) [朱近康 1993 扩展频谱通信及其应用 (北京 中国科学技术出版社)]

[15] Wang S Y, Feng J C 2005 *Journal of Circuits and Systems* **10** 98 (in Chinese) [王世元、冯久超 2005 电路与系统学报 **10** 98]

A method for generating chaotic spread-spectrum sequences and their optimized selection algorithm *

Yu Zhen-Biao　Feng Jiu-Chao†

(*College of Electronic and Information Engineering*, *South China University of Technology*, *Guangzhou* 510641, *China*)

(Received 23 April 2007; revised manuscript received 4 June 2007)

Abstract

A method for generating chaotic spread-spectrum sequences based on the combined chaotic map is proposed. An optimized selection algorithm based on the property requirement of spread-spectrum sequences and the performance index of multiple access interference is also presented. Simulation is performed for the optimized chaotic sequence, and an optimized logistic sequence is applied to a direct sequence spread-spectrum CDMA system under different channel conditions. The results show that the chaotic spread-spectrum sequences generated by the proposed method have similar performance as the logistic spread-spectrum sequences and have better security.

Keywords: CDMA, optimized selection algorithm, Rayleigh fading channel, BER

PACC: 0545

* Project supported by the National Natural Science Foundation of China (Grant No. 60572025); the Program for New Century Excellent Talents in China University (Grant No. NCET-04-0813); the Key Project Foundation of the Education Ministry of China (Grant No. 105137); the Natural Science Foundation of Guangdong Province, China (Grant Nos. 07006496, 04205783).

† Corresponding author. E-mail: fengjc@scut.edu.cn