三元组扩频码在扩频通信中的应用

王 慧[1] 吴成茂[2]
(西安邮电大学研究生院 西安 710061)[1] (西安邮电大学电子工程学院 西安 710121)[2]

摘 要 为了产生、加工出一组逼近白噪声统计信号特性的信号并将其作为扩频码来降低扩频通信系统的误码率、提高可靠性,基于三元组随机数提出三元组扩频码。该扩频码由真随机熵源提供初始值,以多轮重构技术构造背景,通过周期性变轨、控制空间映射和约束判断等方法实现离散轨迹变换,再经均匀映射产生。在不同大小的信噪比和不同幅度的正弦干扰下,采用蒙特卡罗模型仿真测试了三元组、m序列、分段Logistic序列和线性同余序列作为扩频码的直接扩频通信系统的误码率。实验结果表明,三元组扩频码的误码率更低,并且在低信噪比、强衰落、强干扰的情况下也很稳定,可以提高扩频通信系统的抗截获性和抗干扰性,从而保障通信系统的可靠性。

关键词 扩频通信,三元组扩频码,均匀映射,误码率,蒙特卡罗模型
中图法分类号 TN911 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.09.021

Application of Ternary Spread Code in Spread Spectrum Communication

WANG Hui[1] WU Cheng-mao[2]
(Graduate University, Xi'an University of Posts and Telecommunications, Xi'an 710061, China)[1]
(School of Electronic Engineering, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)[2]

Abstract In order to produce, work out a set of signal with approximate white Gaussian noise statistical characteristics, and use it as the spread code to reduce the error rate and improve reliability for the spread spectrum communication system, a novel spread code based on the ternary random sequence was presented. It takes the initial random dynamic element as the initial value, and a multi-round reconstruction method is designed to pretreat a background before using some methods such as periodic orbit-changed, control space mapping and constraint judgment to realize the discrete trajectory transform, what's more, it is producted by uniform mapping. With different SNR and sinusoidal interference, ternary spread sequence's BER was simulated and analyzed as the spread code based on Monte Carlo, so well as m sequence's, piecewise logistic chaotic's and linear congruence pseudorandom sequence. Experimental results demonstrate that ternary spread sequence has lower BER, and it ensures system stability under low signal-to-noise ratio, severes channel attenuation and strong interferences. It could improve anti-intercept ability and anti-jamming ability, and thus guarantee the reliability in spread spectrum communication system.

Keywords Spread spectrum communication, Ternary spread code, Uniform mapping, BER, Monte Carlo model

1 引言

随着民用通信的频带日益拥挤,基于扩频通信发展的CDMA、CDMA2000、WCDMA得到了广泛的应用,扩频通信技术使时间和频带资源得到更好的利用。香农在其文章中指出,在高斯白噪声干扰情况下,在平均功率受限的信道上,实现有效和可靠通信的最佳信号是具有白噪声统计特性的信号。但是对于白噪声信号的产生、加工和复制,迄今为止仍存在着许多技术问题和困难[1]。构造一种逼近白噪声性能的新随机扩频码成为关键,它用来减少由于设备、用户间串扰带来的扩频通信系统的通信质量损失,保持通信的可靠性。

传统的扩频序列是m序列和gold序列,均属于线性反馈移位寄存器序列[2,3]。虽然理论简单且完善,但是其具有周期性且数量有限,不能满足大规模通信系统的要求[4,5]。Logistic、Tent等混沌序列[6,7]的初值敏感性和强随机性,使其也适用于扩频通信。然而由于计算机的计算精度限制,在实际计算中需截取一定长度,从而会导致混沌序列出现周期性[8,9]。同余序列[10,11]也是经常被使用的一种随机序列,有线性同余模型、逆同余模型等。但是同混沌序列一样,具有随机性的只有初值,算法不具有随机性,即初值固定了,序列就固定了[12,13]。以上序列并不能真正更靠近白噪声的随机特性,不适合做扩频序列。所以我们需要寻找一种新的扩频码,来保证扩频通信的可靠性和保密性。

本文基于三元组随机数[14]提出三元组扩频码,其将传统

到稿日期:2013-11-17 返修日期:2014-03-03 本文受国家自然科学基金重点项目(90607008),国家自然科学基金项目(61073106),陕西省教育厅自然科学基金项目(2013JK1129),西安邮电大学研究生创新基金项目(ZL2013-29)资助。

王 慧(1988-),女,硕士生,主要研究方向为扩频通信,E-mail:liuwanghuia@qq.com;吴成茂(1968-),男,高级工程师,硕士生导师,主要研究方向为多媒体信息处理技术及其应用。

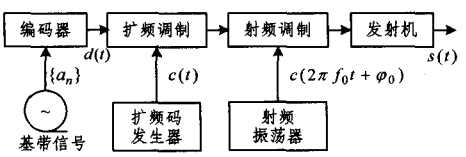
的二元结构扩展为由生成算法、初值和背景空间构成的三元结构。该扩频码是真随机数序列，是建立在用户输入的熵源基础上的随机数序列。该扩频码首先对真随机熵源[15,16]进行多轮重构处理得到满足统计特性需要和规模的背景，由用户输入和系统随机生成的初始值映射为背景上的物理初始地址，然后通过周期性变轨、控制空间映射和约束判断等方法实现离散轨迹变换[17]，再经过同态均匀映射[18]产生。并且已有将三元组随机数应用于图像[19]的加密，并申请获得了专利[20,21]。其作为扩频序列应用于扩频通信，是一种可以提高通信系统的抗截获性、保密性的新型扩频码。本文在不同大小的低信噪比和不同幅度的正弦干扰下，在蒙特卡罗[22,23]直接扩频通信系统中，将三元组扩频码与传统的 m 序列、分段 Logistic 混沌序列和线性同余伪随机序列的误码率进行对比计算，分析可靠性，以得到更适用于扩频通信系统的扩频码。

2 扩频通信系统模型及传统扩频码的产生

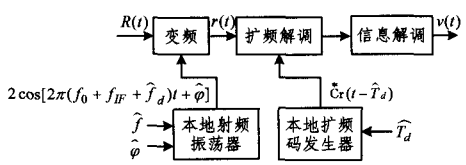
由香农公式 $C=B\log_2(1+\frac{S}{N})$ 可知，在低的信噪比，甚至在信号被噪声淹没的情况下，增加信道带宽后，信道仍可在相同的容量下传送信息，保持可靠的通信。在扩频通信系统中，传输信号的带宽主要由扩频函数决定，此扩频函数通常是伪随机(伪噪声)编码信号。

2.1 扩频通信的物理模型

扩频系统的扩频运算是通过伪随机码或伪随机序列(扩频函数)来实现的。从理论上来讲，用纯随机序列来扩展信号的频谱是最理想的，但是接收端必须复制同一个随机序列。由于随机序列的不可复制性，因此在工程中无法使用纯随机序列，而改为采用伪随机序列。在扩频系统的实际运用中，一般采用易于产生、随机性强、有尽可能长的周期和良好自相关函数、互相关特性的随机序列。常用的伪随机序列有线性反馈移位寄存器序列、混沌序列和同余序列。扩频通信物理模型如图 1 所示。



(a) 发射系统



(b) 接收系统

图 1 扩频通信物理模型

2.2 伪随机扩频码——m 序列

m 序列和 gold 序列是传统的伪随机扩频码，因易于产生且具有一定的随机性而被广泛使用。由于 gold 序列可由两个 m 序列的模 2 和产生，因此本文以 m 序列为例，分析其可靠性。m 序列逻辑结构图如图 2 所示。

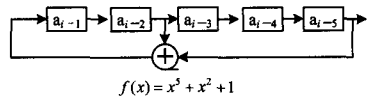


图 2 m 序列逻辑结构图

在初始状态为 00…01 的条件下，线性移位寄存器的序列多项式 $G(x)$ 与特征多项式 $f(x)$ 的关系为：

$$G(x)=\frac{1}{f(x)} \tag{1}$$

m 序列虽然容易产生，自相关性好，但是其互相关特性不理想。m 序列是线性序列，采用线性反馈逻辑，输出序列完全由初始状态和反馈函数唯一确定，容易被敌人破译，即保密性、抗截获性差。m 序列的数目非常有限，且用线性移位寄存器生成的 m 序列长度也是有限的，在实际应用中产生速度慢[4]。m 序列周期不长，第三方易于从扩频码的一小段去重建整个序列，使其可靠性存在一定的风险。选用具有混沌特性的序列作为扩频序列的动态特性会更好[5]。

2.3 伪随机扩频码——分段 Logistic 混沌序列

定义分段 Logistic 混沌映射为：

$$a_{n+1}=\begin{cases}4\mu a_n(0.5-a_n), & 0\leqslant a_n<0.5\\ 1-4\mu(0.5-a_n)(1-a_n), & 0.5\leqslant a_n\leqslant 1\end{cases} \tag{2}$$

其中，$a_0\in(0,1)$，$3.5699456\cdots\leqslant\mu\leqslant 4$。将生成的混沌序列 $\{a_1,a_2\cdots a_n\}$ 转化为二值序列 $\{b_1,b_2\cdots b_n\}$：

$$b_i=\begin{cases}0, & 0\leqslant a_i<0.5\\ 1, & 0.5\leqslant a_i\leqslant 1\end{cases} \tag{3}$$

分段 Logistic 混沌序列曲线关于 x 坐标轴在 0.5 处有对称性，所产生的 0、1 二值序列的平衡度较差。并且混沌序列在计算机上实现的过程中会具有周期性且周期较短。这是由于计算机中数据精度的限制[8,9]。同理，编译器、硬件、软件算法和编程语言都会引起类似的现象[24]。混沌模拟实值序列在传输过程中有无限多个状态，即幅度在[−1，+1]内连续，但却难以准确地实现，混沌多值序列是将混沌模拟实值序列进行量化得到的，降低了随机性[25]。

2.4 伪随机扩频码——线性同余伪随机序列

基于线性同余的伪随机发生器的模型为：

$$X_i=(aX_{i-1}+c)\bmod(M),\ i=1,2,3,\cdots \tag{4}$$

其中，$X_0(0\leqslant X_0<M)$ 为初值，$a(0\leqslant a<M)$ 为乘数，$M(M>0)$ 为模数，通常取 2 的整数次方，以便推导式的取模操作可以用位操作来代替。根据增量 $c(0\leqslant c<M)$ 的不同，又分别称为乘同余法($c=0$)和乘加同余法($c\neq 0$)。

但是，若 X_0、a、M、c 均为整数，则产生的随机数序列 $\{X_n|0\leqslant X_n<M\}$ 也为整数，且 $0\leqslant X_n,X_{n+1}<M$，则由它产生的序列必具有周期性。线性同余随机序列的周期与计算机的字长有关，在整数的尾数字长为 L 位的计算机上，不可能得到周期大于 $2L$ 的均匀随机序列[12]。线性同余算法的强度在于如何将乘数和模数选择好，则产生的序列和从 $1,2,\cdots,m-1$ 中随机选取的序列是不可区分的。但是除了初值 X_0 的选取具有随机性外，算法本身并不具有随机性，因为 X_0 选定后，以后的数就确定性地产生了[13]。

3 基于三元组随机数序列的扩频码——三元组扩频码

三元组随机序列生成中 m 为生成算法，IV 为初始参数，

Key 为用户选择的秘钥空间，则其算法框架可表示为 $KS=(m,IV,Key)$。

三元组随机数序列又称为基于广义信息域离散轨迹变换的随机数序列[17]。广义信息域是所有可以表示为二进制编码的数据所构成的空间 GI，所以三元组扩频码以用户选择广义信息域的信息为熵源，通过多轮重构消除对熵源内容和大小上的依赖，得到满足一定规模且编码出现次数均匀的数据空间——背景 BG。

由用户的任意输入初始信息 u、系统时间戳 t 和系统随机数 r 构成的初始参数 IV，使用 $hash$ 混沌函数消除用户行为相似性的影响，得到泛空间地址 AI。而且引入系统随机生成的 u、t，使得即便用户的输入信息相同，所生成的初始参数 IV 也不同，这是三元组扩频码具有很强的初值敏感性的关键。用轨迹变换参数 DI 分别使 AI 变换为逻辑地址 A，使 A 变为物理地址 ma。ma 为映射在背景 BG 上的物理地址，是初始参数 IV 能在背景 BG 析出随机序列的枢纽。

以物理地址 ma 为始，顺序析出 p 位随机数 M，加入三元组随机数 KS 中。让 AI 逻辑循环 M，得到新的泛空间地址 AI，实现控制空间映射。再通过 D 得到新的物理地址 ma，实现周期性变轨。

在重构背景及生成序列的过程中，用数组记录每个数出现的频次，通过重构约束向量$\vec{c}$与重构约束参数 q 比较，使背景中所有字节编码的出现次数具有良好的统计分布特性；轨迹变换向量$\vec{C}'$和轨迹变换参数 q' 比较，避免了小周期的存在，而且增加了平衡度，实现了约束判断。以周期性变轨、控制空间映射和约束判断等离散轨迹变换为循环，直到得到满足长度的三元组随机数 KS。再将三元组随机数 KS 经过均匀映射，使三元组轨道和获得序列的轨道可以相互拓扑等价，来保证三元组系统最大的动态性。

该扩频码由真随机熵源提供初始值，以多轮重构技术构造背景，通过周期性变轨、控制空间映射和约束判断等方法实现离散轨迹变换，再经均匀映射产生。

3.1 构建三元组扩频码

三元组扩频码将传统的二元结构 $KS=(m,IV)$ 扩展为由生成算法、初值和背景空间构成的三元结构 $KS=(m,IV,Key)$，使每次使用都会产生不用的序列。

$Key=(GI,M,L,D)$ 为用户选择的秘钥空间。用重构初始位置 $M(m_i\in Z^+)$、重构长度 $L(l_i\in Z^+)$ 对用户选择的广义信息 GI（记为 PB_0）经过 S 轮重构生成 PB_S，即 BG（背景）。计数器向量 $c=(c_0,c_1,\cdots,c_{255})$ 中 c_k 是记录每次重构过程中编码 $k\in\{0,1,\cdots,255\}$（k 是 8 位的二进制数）出现的次数。j 是每轮重构的长度，所以每轮重构前 c_k、j 要初始化为零。为使生成的数据空间具有较好的统计分布特性，设置约束参数 q（默认值为 10），使 PB_i 中所有字节编码的出现次数相当。q 越小，PB_i 中编码分布越均匀，约束条件越强。第 i 轮重构生成 PB_i 的框图如图 3 所示。

$IV=(t,v,u)$ 为初始随机动态因子。t、v 由系统生成，分别为系统时间戳和系统随机数，u 为用户输入的初始个性化信息。可见，每次生成的不重复随机的初始点由 IV 决定，也是每次生成不同三元组扩频码的关键决定因素。将初始随机动态因子 IV 经 $hash$ 函数单向映射为一个长度为 $32\times w$bit 的二进制字符串，并分割为 $[32\times w]$ 的向量组，定义为泛空间地址 $AI(x_0,x_1,\cdots,x_{w-1})$。轨迹变换参数 $D=(d_0,d_1,\cdots,d_{w-1})$ 构造地址映射函数，定义了逻辑地址的最大值。为能够保证随机数具有优良的平衡度，设置轨迹变换参数 q'。设每次析出 $p$bit 数据，则 C_k' 是计数器向量 $C'=(C_0',C_1',\cdots,C_{2^p-1}')$ 中记录生成随机数序列过程中编码 $k\in\{0,1,\cdots,2^p-1\}$ 出现的次数，$\vec{C}'$要初始化为零向量，同时通过与 q' 的比较避免了小周期的存在，而且增加了平衡度。生成三元组随机数的算法 m 如图 4 所示。

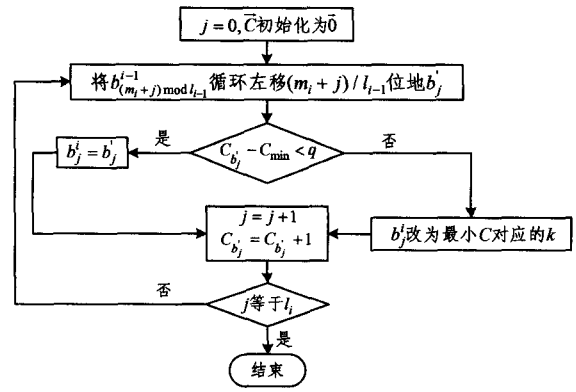


图 3 重构 PB_i 的示意图

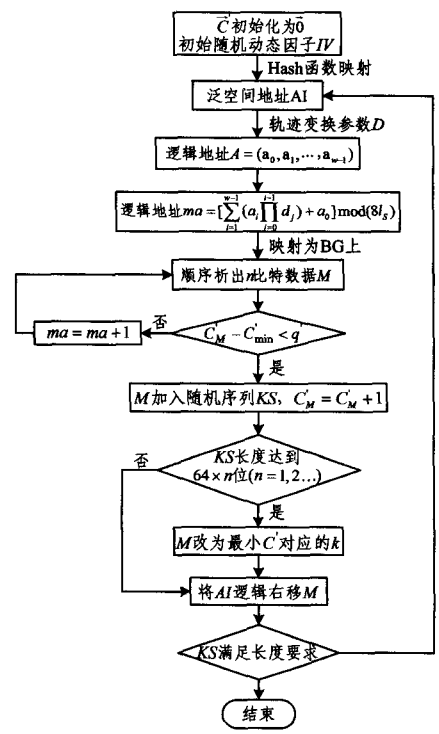


图 4 生成三元组随机数的算法

使用一种同态均匀映射[18]，三元组随机数 KS 变为三元组扩频码 KC，频码具有更强的随机性。

将二值三元组随机数按顺序析出 $l$bit，变为一个十进制数，得到序列 $x_n=\{x_0,x_1,x_2\cdots\}$。若 KS 的长度为 L，则 $\{x_n\}$ 的长度为 $L-l+1$。均匀映射 $g(\cdot)$ 定义为：

$$y_n=g(x_n)=\frac{K(x_n)}{N},n=1,2,\cdots,N \tag{5}$$

其中，N 是 $\{x_n\}$ 的长度，$K(x_n)$ 是 x_n 在 $\{x_n\}$ 中按升序排列的

序号。将实值序列转换为二值序列，引入转换函数 $T(\cdot)$ 为：

$$s(n)=T(y_n)=\begin{cases}-1, & y_n\in\bigcup_{d=1}^{m}B_{2d-1}^{2m}\\ 1, & y_n\in\bigcup_{d=1}^{m}B_{2d}^{2m}\end{cases} \tag{6}$$

其中，$2m$ 是正整数，B_0^{2m}，B_1^{2m}，B_2^{2m}，…，B_{2m}^{2m} 是在[0,1]上连续相等的 $2m$ 子区间。$s(n)$ 即为三元组扩频码 KC。

3.2 三元组扩频码的性质

扩频通信的基本特点的传输信息所用的信号带宽远大于信息本身的带宽，而传输信号的带宽主要由扩频函数决定，所以扩频码序列应具有尽可能长的周期，使第三方难以从扩频码的一小段去重建整个码序列。而三元组扩频码将$\vec{C}'$与q'比较，当序列长度为 64 整数倍时更改当前编码的约束控制和周期性变轨控制，使序列具有周期不重复性[14]。

引入基于用户 U 盘、手机、计算机等电子设备中存储的数字信息的广义信息域，作为三元组随机序列的熵源空间，使得随机序列具有真随机性，更不可预测。即使用户的输入初始信息相同，与系统自动生成的随机数和系统时间戳经 *hash* 函数共同映射后，得到的初始参数也会不同，并通过反馈迭代机制可输出大量完全不相关的序列，其具有初值敏感性。

由于三元组扩频码对初始条件极为敏感，两个几乎相同的系统即使处于完全相同的用户初始值也会迅速变成为完全不同的状态。同时增加了系统的抗碰撞性，消除了用户输入初始值的重复性或相似性的影响。

经理论分析和实验证明，同态均匀映射适合所有具有混沌特性的序列，使序列具有更好的随机性、平衡性、自相关和互相关性，并且扩宽了系数空间。

三元组随机数的生成速度不受用户选择的广义信息 *GI* 影响，且其平均产生速度达到 9MB/s[14,17]；且同态均匀映射的算法并不复杂，计算速度快[18]。选择不同 *GI* 生成三元组扩频码的平均速度也可达到 8.8MB/s 以上，所以三元组扩频码的编码效率能够满足实际应用需要。

三元组扩频码由用户输入和系统随机生成数经 hash 映射提供初始值，实现初值的随机性；然后通过周期性变轨、控制空间映射和约束判断等离散轨迹变换的方法[17]，实现算法的随机性。相比于混沌序列只有初值和算法初值具有随机性，三元组扩频码具有更强的随机性，不易于破解，可以提高通信系统的保密性，以及可靠性和安全性。

经验证，三元组扩频码具有良好的初值敏感性、周期不重复性、平衡度、混沌特性、抗对抗性和强随机性，通过了严格的 NIST SP800-22 随机性测试，逼近高斯白噪声的统计特性。综上，三元组扩频码适合作为扩频通信系统的扩频随机序列，能降低通信系统的误码率，提高可靠性和保密性。

4 三元组扩频码的误码率分析与仿真

为了检验三元组扩频码作为扩频码提高扩频通信可靠性的效果，在蒙特卡罗扩频通信系统仿真模型中使用三元组扩频码，检测其误码率，并检测 m 序列和分段 Logistic 混沌序列在相同条件下的误码率，与使用三元组扩频码的系统的误码率进行对比。蒙特卡罗仿真的直扩扩频系统框图如图 5 所示。对误码概率的估计是误码率，误码概率[26]为：

$$P_b=Q\sqrt{2E_b/N_0} \tag{7}$$

其中，N_0 为单边噪声功率谱密度；E_b 为符号能量；$Q(x)$ 为高斯 Q 函数。

$$Q(x)=\frac{1}{2\pi}\int_x^{\infty}\exp\left(-\frac{1}{2}y^2\right)\mathrm{d}y \tag{8}$$

在数字通信系统中，传输的可靠性是用信息传输的差错率来描述的，即衡量收到的信息与发出的信息之间的符合程度。所以，扩频通信系统的实际误码率[27]为：

$$Pe=\frac{E_n}{NUM} \tag{9}$$

其中，E_n 为传输出现错误的码的数目，NUM 为传输的码的总数目。

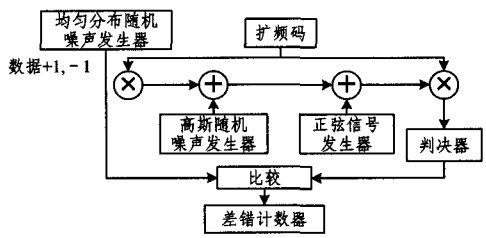


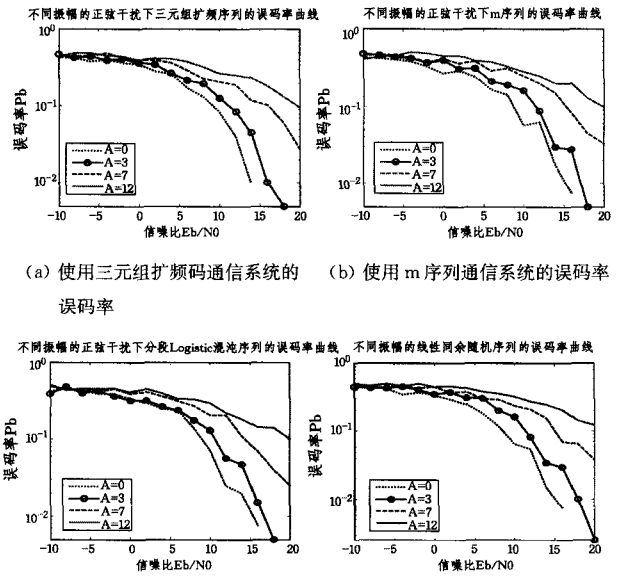
图 5 蒙特卡罗仿真的直扩扩频系统框图

表 1 不同幅度干扰下的误码率

幅度 信噪比	A=0				A=3				A=7				A=12			
	三元组序列	m 序列	分段 Logistic	线性同余序列	三元组序列	m 序列	分段 Logistic	线性同余序列	三元组序列	m 序列	分段 Logistic	线性同余序列	三元组序列	m 序列	分段 Logistic	线性同余序列
−10	0.3238	0.3219	0.3301	0.3196	0.3331	0.3681	0.3593	0.3680	0.3639	0.4080	0.3968	0.4091	0.3984	0.4331	0.4359	0.4308
−8	0.2905	0.2900	0.2856	0.2921	0.3059	0.3303	0.3226	0.3335	0.3363	0.3821	0.3729	0.3896	0.3761	0.4074	0.4240	0.4169
−6	0.2405	0.2421	0.2385	0.2384	0.2516	0.2895	0.2799	0.2879	0.2924	0.3543	0.3419	0.3510	0.3370	0.3861	0.3914	0.3975
−4	0.1875	0.1834	0.1776	0.1843	0.2020	0.2500	0.2334	0.2501	0.2548	0.3126	0.3091	0.3390	0.3048	0.3596	0.3491	0.3789
−2	0.1308	0.1339	0.1219	0.1303	0.1541	0.1934	0.1770	0.1949	0.2073	0.2806	0.2685	0.2888	0.2638	0.3396	0.3171	0.3378
0	0.0790	0.0758	0.0835	0.0800	0.1020	0.1385	0.1320	0.1403	0.1535	0.2304	0.2180	0.2405	0.2189	0.2986	0.2819	0.3123
2	0.0393	0.0378	0.0356	0.0375	0.0523	0.0903	0.0825	0.0919	0.0983	0.1851	0.1688	0.1898	0.1624	0.2503	0.2390	0.2628
4	0.0114	0.0098	0.0133	0.0119	0.0208	0.0409	0.0416	0.0501	0.0574	0.1371	0.1294	0.1495	0.1173	0.2256	0.2028	0.2244
6	0.0039	0.0016	0.0023	0.0023	0.0049	0.0160	0.0146	0.0225	0.0258	0.0941	0.0804	0.1016	0.0733	0.1735	0.1609	0.1879
8	0.0001	0.0001	0.0004	0.0000	0.0006	0.0048	0.0041	0.0071	0.0096	0.0565	0.0489	0.0716	0.0413	0.1329	0.1123	0.1445
10	0.0000	0.0000	0.0000	0.0000	0.0001	0.0003	0.0011	0.0019	0.0029	0.0261	0.0220	0.0381	0.0220	0.0989	0.0808	0.1060
12	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0001	0.0004	0.0105	0.0095	0.0171	0.0078	0.0605	0.0459	0.0685
14	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0004	0.0023	0.0023	0.0056	0.0020	0.0311	0.0259	0.0433
16	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0003	0.0003	0.0010	0.0005	0.0109	0.0115	0.0240
18	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0005	0.0031	0.0024	0.0096
20	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0004	0.0005	0.0016

为了更多方面地分析扩频码的适用性，在蒙特卡洛直扩模型中，分析比较了在不同幅度的正弦干扰下每种扩频码在不同信噪比下的误码率变化情况。在不同信噪比下，信号经扩频后发送，在信道中叠加方差为 $\sigma^2=N_0/2$ 的高斯白噪声和形式为 $i(n)=A\sin\omega_0 n$ 的正弦干扰，其中 $0<\omega_0<\pi$，且仿真中令 $A=0,3,7,12$。接收到的信号经解调解扩后进行输出判决，然后对获得的输出序列与原输入信号进行对比，计算误码率。图 6 是通过 MATLAB 软件仿真的结果。为消除偶然性，取 100 次的结果取平均，如表 1 所列。

由图 6 分析：随着信噪比的提高，所有扩频码的扩频通信系统误码率均降低；在增大正弦干扰幅度下，相同扩频码的通信系统的误码率有所增加。



(a) 使用三元组扩频码通信系统的误码率　(b) 使用 m 序列通信系统的误码率

(c) 使用分段 Logistic 混沌序列通信系统的误码率　(d) 使用线性伪随机序列通信系统的误码率

图 6　不同幅度干扰的误码率

分析表 1 可知，在正弦干扰幅度为零时，即只有高斯白噪声的情况下，4 种扩频码的误码率相当。在相同信噪比和相同幅度的正弦干扰下，三元组扩频码的误码率是最低的，并随着信噪比的提高，误码率保持相对快速、平稳的下降，明显优于其他 3 种序列。接下来，性能较好的是分段 Logistic 混沌序列和 m 序列，最差的是线性同余序列。且随着正弦干扰幅度的增加，三元组扩频码对误码率降低的改善越为明显。综上，三元组扩频码用于扩频通信系统时，在不同幅度的正弦干扰、不同大小的信噪比下，甚至信号被噪声淹没，都能保证其很低的误码率和通信系统的可靠性。

结束语　虽然基于 m 序列、分段 Logistic 混沌序列和线性同余序列的伪随机扩频码可以用来扩展发送序列频谱的带宽，但它们均为貌似随机的伪随机信号，具有确定性。所以三元组扩频码作为一种新颖的扩频码，引入真随机熵源，具有更强的不可分析和不可预测性，逼近白噪声的性能，更适合作扩频码[28]。三元组扩频码的数目众多，可以满足日益增长的用户量的需求，是可以符合构造数目大、性能好的扩频码的迫切需要的。且其由用户输入和系统随机产生的数共同提供初始值，具有更大的不确定性，实现初值的随机性；然后通过周期性变轨、控制空间映射和约束判断等离散轨迹变换的方法，实现算法的随机性。相比于混沌序列只有初值和算法初值具有随机性，三元组扩频码的初值和算法均具有随机性，既可以提高抗累计扩频码的能力，也可以提高序列的安全性和保密性。

三元组随机数序列是一种新的随机数序列体系，申请并被授权了国家发明专利[29]。本文基于三元组随机数序列提出三元组扩频码，其模式和体质是有创新意义的，并有很大的应用价值。三元组扩频码具有良好的平衡度、初值敏感性、周期不重复性、混沌特性、抗对抗性和强随机性，其统计特性更贴近于白噪声。在不同的信噪比和不同幅度的干扰下，分析得到三元组扩频码应用在扩频通行系统中的误码率更低，越大的干扰，误码率的改善效果越好，能抵抗强的干扰噪声，更能满足扩频通信系统对可靠性的要求。因此，使用三元组随机数模型构造扩频序列，在扩频通信系统中是可行的，并且具有实际的应用价值。

参 考 文 献

[1] 田日才. 扩频通信[M]. 北京：清华大学出版社，2007

[2] 张重阳. CDMA 系统伪码序列的相关性分析与仿真研究[J]. 通信技术，2008，41(9)：94-96

[3] Zheng Da-guo, Wang Gang, Li Bo, et al. An improved pseudo random sequence based on the m-sequence[C] // Cross Strait Quad-Regional Radio Science and Wireless Technology Conference (CSQRWC), 2011. IEEE, 2011, 2: 881-884

[4] 李雪松. 混沌扩频通信系统及其干扰技术研究[D]. 成都：电子科技大学，2009

[5] 郭杰，王琳，李秉智. Chebyshev 混沌序列和 m 序列的特性比较和分析[J]. 重庆邮电学院学报，1999，11(4)：30-33

[6] 范九伦，张雪锋. 分段 Logistic 混沌映射及其性能分析[J]. 电子学报，2009，37(4)：720-725

[7] Yang Qi-lun, Zhang Yun-hua, Gu Xiang. A Signal Model Based on Combination Chaotic Map for Noise Radar[J]. Progress In Electromagnetics Research M, 2013, 28: 57-71

[8] Adler R L, Rivlin T J. Ergodic and mixing properties of chebyshev polynomials [J]. Proceeding of the American Mathematical Society, 1964, 15: 794-796

[9] Dellago C, Hoover W G. Finite-precision stationary states at and away from equilibrium[J]. Physical Review E, 2000, 62(5): 6275-6281

[10] Brown Forrest B, Yasunobu N. The MCNP5 random number generator[J]. Transactions of the American Nuclear Society, 2002, 87: 230-232

[11] 马华，张晓清，张鹏鸽. 一种基于线性同余算法的伪随机数产生器[J]. 纯粹数学与应用数学，2005，12(3)：206-209

[12] 周燕. 关于线性同余组合发生器的周期性和统计性质[J]. 重庆大学学报：自然科学版，2000，23(6)：69-70

[13] 沈华韵，张鹏，王侃. 改进线性同余法随机数发生器[J]. 清华大学学报：自然版，2009，49(2)：191-193

（下转第 131 页）

[4] Newman M E J, Girvan M. Finding and evaluating community structure in networks[J]. Phys. Rev. E, 2004, 69: 026113

[5] Li H J, Zhang X S. Analysis of stability of community structure across multiple hierarchical levels[J]. Europhys. Lett., 2013, 103: 58002

[6] Li H J, Wang Y, Wu L Y, et al. Community structure detection based on potts model and spectral characterization[J]. Europhys. Lett., 2012, 97: 48005

[7] Li H J, Wang Y, Wu L Y, et al. Potts model based on a Markov process computation solves the community structure problem effectively[J]. Phys. Rev. E, 2012, 86: 016109

[8] Muff S, Rao F, Caflisch A. Local modularity measure for network clusterizations[J]. Phys. Rev. E, 2005, 72(5): 056107

[9] Gregory S. Finding Overlapping Communities Using Disjoint Community Detection Algorithms[M] // Complex Networks. Springer Berlin Heidelberg, 2009: 47-61

[10] Palla G, Derenyi I, Farkas I, et al. Uncovering the overlapping community structure of complex networks in nature and society [J]. Nature, 2005, 435: 814-818

[11] 沈华伟,程学旗,陈海强,等. 基于信息瓶颈的社区发现[J]. 计算机学报, 2008, 31(4): 677-686

[12] Raghavan U, Albert R, Kumara S. Near linear time algorithm to detect community structures in large-scale networks[J]. Phys. Rev. E, 2007, 76(3): 036106

[13] Pujol J M, Bejar J, Delgado J. Clustering algorithm for determining community structure in large networks[J]. Phys. Rev. E, 2006, 74(1): 016107

[14] 王观玉. 基于聚类的复杂网络社团发现算法[J]. 计算机工程, 2011, 37(10): 58-60

[15] 杨博,刘大有,金弟,等. 复杂网络聚类方法[J]. 软件学报, 2009, 20(1): 54-66

[16] Noh J, Rieger H. Random walks on complex networks [J]. Phys. Rev. Lett., 2004, 92(11): 118701

[17] Lai D, Lu H, Nardini C. Enhanced modularity-based community detection by random walk network preprocessing [J]. Phys. Rev. E, 2010, 81(6): 066118

[18] Ravasz E, Barabasi A L. Hierarchical organization in complex networks[J]. Phys. Rev. E, 2003, 67: 026112

[19] Baras J S, Hovareshti P. Efficient and robust communication topologies for distributed decision making in networked systems [C] // Proceedings of 47th IEEE Conference on Decision and Control. 2008: 2973-2978

[20] Danon L, Duch J, Guilera D, et al. Comparing community structure identification[J]. J. Stat. Mech., 2005, 29: 09008

[21] Blondel V D, Guillaume J L, Lambiotte R, et al. Fast unfolding of communities in large networks[J]. J. Stat. Mech., 2008, 10: 10008

[22] Rosvall M, Bergstrom C T. Maps of random walks on complex networks reveal community structure [J]. Proc. Natl. Acad. Sci., 2008, 105(4): 1118-1123

[23] Zachary W W. An information flow model for conflict and fission in small groups[J]. Journal of Anthropological Research, 1977, 33: 452-473

[24] Huh W, et al. Global analysis of protein localization in budding yeast[J]. Nature, 2003, 425: 686-691

[25] Jansen R, Gerstein M. Analyzing protein function on a genomic scale: the importance of gold-standard positives and negatives for network prediction[J]. Current Opinion in Microbiology, 2004, 7: 535-545

[26] Ruepp A, et al. The FunCat, a functional annotation scheme for systematic classification of proteins from whole genome[J]. Nucleic Acids Res, 2004, 32: 5539-5545

(上接第 114 页)

[14] 张国基,李璇,刘清,等. 基于广义信息域离散轨迹变换的随机数生成器[J]. 物理学报, 2012, 61(6): 0605021-0605029

[15] 董俊,朱文,蒲秀英,等. 物理真随机数发生器的设计[J]. 电光与控制, 2013, 20(2): 93-96

[16] 周庆,胡月,廖晓峰. 基于鼠标轨迹和混沌系统的真随机数产生器研究[J]. 物理报, 2008, 57(9): 5413-5418

[17] 李璇. 三元组密钥流发生器的机理及应用研究[D]. 广州: 华南理工大学, 2012

[18] Wang Fu-lai. A universal algorithm to generate preudo-random numbers based on uniform mapping as homemophism[J]. Chin. Phys. B., 2010, 19(9): 0905051-0905056

[19] Li Xuan, Zhang Guo-ji, Liao Yu-liang. Chaos-based true random number generator using image[J]. InternationalConference on Computer Science and Service System, 2011, 6(3): 2145-2147

[20] 张国基,徐浩,黎凤鸣. 基于广义信息域的高级加密系统及方法: 中华人民共和国, CN 101394268 B[P]. 2011. 05. 18

[21] 张国基,刘清,黎凤鸣,等. 基于广义信息域的动态加解密方法: 中华人民共和国, CN 101383703 B[P]. 2011. 04. 27

[22] 冯富强,陈举鹏. 在低信噪比条件下 DS-DS 信号的检测和参数估计[J]. 通信学报, 2002, 23(9): 63-68

[23] 贾志成,蒋文娟,李建娜. 基于蒙特卡罗的扩频通信仿真与分析[J]. 通信技术, 2007, 28(8A): 206-209

[24] Palmore J. Computer arithmetic, Chaos and Fractals [J]. Physical D., 1990, 42(1): 99-110

[25] 王亚东. 混沌序列在扩频通信中的研究与应用[D]. 西安: 西安电子科技大学, 2007

[26] 曾璐,谢晓尧. 基于 MATLAB 扩频通信系统误码率的研究[J]. 通信技术, 2011, 44(11): 25-29

[27] 吴成茂,李杜鹃,王保平. 混沌扩频通信及其误码率[J]. 西安邮电大学学报, 2013, 18(3): 10-13

[28] 黄乘顺,李星亮. 基于混沌的扩频通信系统及性能分析[J]. 通信技术, 2008, 41(12): 37-39

[29] 张国基,刘清,黎凤鸣,等. 基于广义信息域的伪随机码发生器及其发生方法: 中华人民共和国, CN 101364868 B[P]. 2012. 02. 01