维普资讯 http://www.cqvip.com

小波分析在信息安全之真随机数发生器中的应用*)

Application of Wavelet Analysis in Random Number Generators of the Information Security

吕述望　苏桂平　杨　柱　薛英花

(中国科学院研究生院信息安全国家重点实验室　北京100039)

Abstract We analyze the some random number generators used in information security currently, apply the decomposition and reconstruction of wavelet analysis to random number generator to raise the quality of true random number and meet cryptographic technology.

Keywords Wavelet transform, Information security, Noise signal, Random number

1. 引言

密码技术对随机数的要求较高,它要求的真正的随机数序列应具有如下三个特点:

(1)看起来是随机的:能通过频数检验、跟随特性检验、游程检验、扑克检验等基本的统计特性检验。

(2)不可预测:即使给出产生序列的硬件和所有以前产生的序列的全部知识,也不可能预测下一个随机位是什么。

(3)不能重复产生:在完全相同的条件下,将得到两个不相关的随机序列。

真随机数在密码技术中是非常重要的,比如密钥管理、众多的密码学协议、数字签名和身份认证等都要用到真随机数。随着网络技术的广泛利用,信息安全变得非常重要。如何方便、快速产生统计特性良好的真随机数已成为信息安全领域的一个重要研究课题,本文介绍如何利用小波分析理论获得真正噪声信号,从而得到高质量的随机数。

2. 随机数发生器的噪声信号分析

正如著名应用密码学家 Schneier B. 所说:采集大量随机数的最好方法是选取真实世界的自然随机性[1]。所以关于真随机数发生器,在国内外已有很多这方面的研究。其中不少是利用各种噪声做成的随机数发生器。现介绍几种利用如下:

(1)Linux 操作系统中产生真随机数随机位的工作原理为:随机数源的获取有如下4种方式:键盘随机性、鼠标随机性、中断随机性、块设备随机性。不同的获取方式每次会获得适合的随机位,为提取随机性,这些得到的随机位被存放在一个缓存区中。如何去掉相关性和偏差得到真正的随机数,也是值得讨论的。

(2)在文[2]中介绍利用计算机磁盘驱动器的随机数发生器,磁盘的偏差主要是空气震荡的噪声引起的,测量读取磁盘扇区的时间,利用时间差作为随机数源。

(3)在文[3]中,INTEL 利用半导体内部的噪声内部的热噪声、闪烁噪声、结噪声等噪声信号作为噪声源,对它们混合输出的信号进行采样,来产生真随机数。

(4)在文[4]中介绍 AT&T 公司的随机数发生器是基于自激震荡器中噪声,引起频率的不稳定,对这种不稳定的频率信号进行采样,以此作为随机序列。

(5)在文[5]中介绍利用通讯线路和网络线路的噪声产生随机数。主要问题是如何从线路传送的信号中取出噪声信号。

(6)我们中国科学院信息安全国家重点实验室利用模拟和数字电路的各种噪声成功研制了数字物理噪声源芯片,产生信息安全需要的真随机序列[6]。

在以上的随机数发生器中有一个共同的问题是:如何去掉偏差和相关性,如何滤掉周期或定时信号,从而得到统计特性良好的真随机序列。在文[2]中用快速傅立叶变换解决了部分问题,但不够全面,也缺少通用性。下面讨论如何利用小波分析这一新的数学工具去解决这个问题。

3. 小波变换与多分辨分析原理

3.1 小波变换

小波分析是一种时、频多分辨率分析方法,是傅立叶分析发展史上的一座里程碑。傅立叶分析能用到的地方,小波分析同样适用。

定义1(小波函数)　小波函数 $\Psi(t)$ 指具有震荡特性、能迅速衰减到零的一类函数。通过 $\Psi(t)$ 的伸缩和平移后派生出一族函数 $\Psi_{a,b}(t)$:

$$\Psi_{a,b}(t)=|a|^{-1/2}\Psi(t-b/a)\quad b\in R,a\in R,a\neq 0 \qquad (1)$$

式中,$\Psi_{a,b}(t)$ 称连续小波,a 为尺度因子或频率因子,b 为时间因子。

若 $\Psi_{a,b}(t)$ 满足式(1),对于能量有限信号或时间序列 $f(t)\in L^2(R)$,其连续小波变换定义为:

$$W_\Psi f(a,b)=\langle f,\Psi_{a,b}\rangle=|a|^{-1/2}\int f(t)\overline{(t-b/a)}dt \qquad (2)$$

式中,$\overline{(t)}$ 为 $\Psi(t)$ 的复共轭函数。式(2)说明小波变换是对 $f(t)$ 按不同尺度进行分解。

小波分析中的正交函数系是在选择适当的基本小波(母波)后,通过伸缩和平移来产生其"小波"。小波分析相当于一个数学显微镜,具有放大、缩小和平移功能。

在实际应用中,时间序列大多是离散的,因此,必须用与之匹配的离散小波变换对时间序列进行分解与重构。比如:在常用的二进小波中,选 $a=1/2^j$, $b=k/2^j$,常将连续小波变换离散化。

3.2 小波分解与重构

定义2(多分辨分析)　空间 $L^2(R)$ 中的多分辨分析是指 $L^2(R)$ 中满足如下条件的一个空间序列 $\{V_j\}_{j\in Z}$:

*)本文受国家重点基础研究发展规划项目(编号:G1999035808)资助。吕述望　教授,博士生导师。苏桂平　博士生。杨　柱　硕士生。薛英花　硕士生。

维普资讯 http://www.cqvip.com

(1)单调性:$V_j \subset V_{j+1}$,对任意 $j \in Z$;

(2)逼近性:$\bigcap V_j = \{0\}$,集中 $j \in Z$,close$\{\bigcup V_j\} = L^2(R)$,j 取值从$(-\infty, \infty)$;

(3)伸缩性:$f(t) \in V_j \Leftrightarrow f(2t) \in V_{j+1}$,伸缩性体现了尺度的变化、逼近正交小波函数的变化和空间的变化具有一致性;

(4)平移不变性。对任意 $k \in Z$,有 $\phi(2^{-j/2}t) \in V_j \Rightarrow \phi(2^{-j/2}t - k) \in V_j$;

(5)Riesz 基存在性:存在 $\phi(t) \in V_0$,使得$\{\phi(2^{-j/2}t - k) | k \in Z\}$构成 V_j 的 Riesz 基。

定理1 存在 $\phi(t) \in V_0$,使它的整数平移系$\{\phi(2^{-j/2}t - k) | k \in Z\}$构成 V_j 的规范正交基。

定理证明略,可参看参考文[7]。

设 V_j 表示信号 S 分解的低频部分 A_j,W_j 表示分解的高频部分 D_j,则 W_j 是 V_j 在 V_{j+1}中的正交补,即 $V_j \oplus W_j = V_{j+1}$,$j \in Z$,显然 $V_j \oplus W_j \oplus W_{j+1} \oplus \cdots \oplus W_{j+m} = V_{j+m}$,则多分辨分析的子空间 V_0可以用有限个子空间来逼近,即有:

$$V_0 = V_1 \oplus W_1 = V_2 \oplus W_2 \oplus W_1 = \cdots = V_n \oplus W_n \oplus W_{n-1} \oplus \cdots \oplus W_2 \oplus W_1 \quad (3)$$

若令 $f_j \in V_j$ 代表分辨率为 2^{-j}的函数 $f \in L^2(R)$的低频部分,$d_j \in W_j$ 代表函数的高频部分,则式(3)意味着:

$$f_0 = f_1 + f_d = f_2 + d_2 + d_1 = \cdots = f_n + d_n + d_{n-1} + \cdots d_2 + d_1$$

注意 $f = f_0$,这表明:任何函数 $f \in L^2(R)$都可以根据分辨率为 2^{-n}的低频部分和分辨率为$2^{-j}(1 < \leqslant j \leqslant n)$的高频部分完全重构。

4 小波分析在随机数发生器中的应用

4.1 用小波分析得到噪声信号

小波分析作为一种新型的时、频域分析工具,它给信号加了一个时-频窗口,可根据频率自动调节窗口的大小,在时、频域同时具有良好的局部化性质,易于捕捉和分析微弱信号和突变信号,在分析噪声信号方面有广阔的应用前景。

在实际工程中,周期信号或有用信号通常表现为低频信号,噪声信号通常表现为高频信号。若要得到噪声,可对信号进行以下处理:先对信号 S 进行小波分析,如进行三层分解,分析过程如图1。

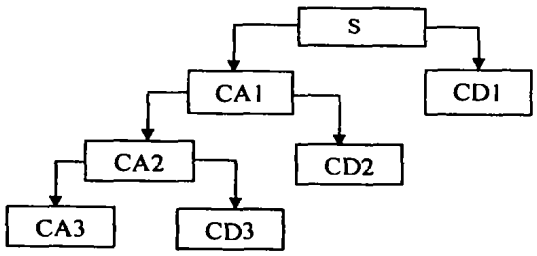

图1

噪声通常包含在高频部分 CD1,CD2,CD3,…中,把低频部分置零,然后对信号重构,滤掉周期和固定信号,得到噪声信号。利用小波变换的多分辨率性质,基于信号和随机噪声在小波变换域中不同的模极大值系数特征,能提取信号和噪声在多尺度分辨空间中的波形特征。保持对信号波形细节的较好分辨率,因此在对非平稳信号的时变处理中具有自身的优越性。

小波分析是一种全新的时频分析方法,傅里叶分析用一种数作为基函数来逼近任意信号思想,小波分析的基函数是一系列尺度可变函数。这使得小波分析具有良好的时频定位特性以及对信号的自适应能力,所以能够对各种时变信号进行有效的分解。

4.2 用小波分析提取噪声信号的程序清单

MATLAB 是一套高性能的数值计算和可视化软件。下面用该软件工具库函数对提取噪声信号的过程进行编程。程序清单如下:

```
%采集的信号按照 MATLAB 格式存成 MAT 文件,文件名为 signal1.mat
    load signal1; %将信号装入 MATLAB 工作环境
s=signal1(1,5000); %取采样信号的前1-5000点,具体多少点可任意定
ls=length(s); %计算采样序列长度
[c,l]=wavedec(s,3,'db1'); %采用 db1小波并对信号进行三层分解
cd1=detcoef(c,l,1); %提取第一层的高频系数
cd2=detcoef(c,l,2); %提取第二层的高频系数
cd3=detcoef(c,l,3); %提取第三层的高频系数
%对分解结构[c,l]中的各层高频部分进行重构
for i=1:3
  decmp=wrcoef('d',c,l,'db1',4-i);
```

在去掉周期和固定信号后,得到完全随机的噪声信号。然后对噪声信号进行采样,可以得到我们需要的随机序列。这种随机序列当然是难以预测和不相关的,可以更好地满足信息安全对序列随机性的要求。

小结 从分辨率看,小波变换较好地解决了时间和频率分辨率的矛盾,与加窗傅里叶变换不同,小波变换的窗宽(基宽度)是可变的,它在高频时使用短窗口,而在低频时则使用宽窗口,这充分体现了相对带宽频率分析和自适应分辨分析的思想,它与时变信号特性也是一致的,用以分析时变信号十分有效,这也是有人将其称为"数学显微镜"的原因。

小波分析可对信号进行多尺度分析,具有很强的特征提取功能,对突变信号的处理优势尤为明显。由于随机噪声信号的小波变换与有效信号的小波变换在特征上具有明显的区别,因此小波分析方法在信息安全中随机数发生器的研制方面可以得到广泛的应用。

参 考 文 献

1 Schneier B. Applied Crytography. Jone Wiley & Sons,1994

2 Davis D, Ihaka R, Fenstermacher P. Crytographic Randomness from Air Turbulence in Disk Drive. Advances in Cryptology-CRYPTO'94 Proceedings, Springer_Verlag, 1994. 114～120

3 Benjamin J, Paul K. The Inter Random Number Generator. http://www.cryptography.com

4 AT&T. T7001 Random Number Generator. Data sheet, Aug. 1986

5 Venkatesan S, Anantharam V. The Common Randomness Capacity of a Network of Discrete Memoryless Channels. IEEE Trans. Inform. Theory, 2000, 46(2): 367～387

6 相曙华. 数字物理噪声源及其芯片集成:[中国科学技术大学研究生院硕士论文]. 1998

7 崔锦泰. 小波分析导论. 西安:西安交通大学出版社, 1995. 1

8 基于 MATLAB 的系统分析与设计(小波分析). 西安:西安电子科技大学出版社, 1999, 12