国防科技大学学报
JOURNAL OF NATIONAL UNIVERSITY OF DEFENSE TECHNOLOGY
第19卷第1期 1997年2月 Vol. 19 No. 1

一种实用的有线电视加解扰方案*

贾 平 邝 明
(国防科技大学电子技术系 长沙 410073)

摘 要 在分析了电视加扰技术中的模拟加扰方式和数字加扰方式后，对数字加扰时基处理中的行旋转、行置换、行变换等方法做了详细分析；为了保护有线电视加扰系统的安全，采用了随机数的产生、数据的加密等技术。最后详细介绍了一个包括加、解扰系统和用户控制的实验系统。

关键词 有线电视，加扰，行旋转，行置换，行变换，加密
分类号 TN918.7

A Practical Scheme on the Scrambling and the Descrambling of CATV

Jia Ping Kuang Ming
(Department of Electronic Technology, NUDT, Changsha, 410073)

Abstract After analying the analogic and digital scrambling ways, line rotation scrambling, line jitter scrambling, line permutation ways of digital scrambling processing are discussed in detail. In order to protect CATV scrambling system, random number generator and data encryption techniques are used. At the end of the paper, an experimental system is described which includes the scrambling system, descrambling system and the controls of users.

Key words CATV, scrambling, line rotation scrambling, line jitter scrembling, line permutstion, encryption.

1 加解扰技术简介

1.1 CATV 加密系统的构成

在 CATV 加密系统中，把信号进行加扰后播出，只有持有解扰器、交给密钥的用户才能接收。一个 CATV 加密系统的组成主要包括加扰器、用户管理器、密码控制和解扰器

* 1996年3月4日收稿

等几部分。

首先, 广播信号用加扰器加扰后发送, 用解扰器进行解扰。当用固定不变的方式进行加扰时, 通过观测被加扰的信号, 读出加扰方法, 在接收器下功夫, 会产生非授权接收的危险。因此, 要采用伪随机 (PN) 信号, 在短时间内变化加扰参数。这样就很难从波形上推断出加扰的方法及参数。

其次, 在接收端, 产生与发射端相同的 PN 信号序列, 同时, 发射端将 PN 序列的初值作为加扰钥匙 (称为 K_s), 发送给接收机, 以实现正确的解扰。这种加扰钥匙由于时时刻刻都在变化, 所以必须随加扰的广播信号一起发送。

由于这种加扰钥匙 (K_s) 随电波传播, 为了避免他人知道这种钥匙, 必须经过密码化以后发送。密码化的钥匙, 称为工作密钥(K_w)。工作密钥没有必要进行频繁的变化, 例如, 用一个月左右的间隔更新一次就够了。另外, 这种工作密钥能用电波、磁卡及 IC 卡等物理媒介体、或电话线等传送。

1. 2 电视图像信号的加扰

对图像的加扰方式主要分为模拟信号加扰和数字信号加扰两大类。

作为图像加扰方式, 在 CATV 发展的初期, 多采用的是同步抑制与极性反转的方式, 其实现电路简单, 但保密性、安全性及图像还原性都较差。随着时基处理技术的采用和数字电路技术的发展, 现在的图像加扰方式大多采用了将电视信号数字化进行时基加扰的方式。

数字加扰的主要思想是将电视信号数字化后存储在存储器中, 然后改变其取出数据的顺序, 再经 D/A 转换后送到模拟传输线上。数字加扰又可分为行旋转、行置换、行变换三种方式, 图像信号多采用行旋转与行变换方式进行加扰, 也可两者并用。

行旋转方式是在扫描行内设置伪随机切割点, 在切割点前后进行改换输出的方式, 将在水平方向上扰乱画面。

行置换方式是把扫描行的顺序进行改换的方式, 在垂直方向扰乱画面。改换的顺序由伪随机数来指定。

行变换方式是挪动时分复用数字信号或图像信号相对于同步信号的位置, 把图像信号与同步信号的相对位置加以扰乱的方式。复用位置以伪随机数控制。

1. 3 数据的传输

数据的传输主要包括 PN 产生器的初始值 K_s, 工作密解 K_w, 用户信息 (是否合法用户) 及设备寻址等。这些数据的传送大多通过电视多工广播系统。

电视多工广播是指在普通电视广播中附加传送新信息的广播系统。可利用频分多工和时分多工通过信道复用来实现。其中使用较多的是场消隐期间 (VBI) 的图文广播和行消隐期间 (HBI) 的多路伴音广播。

2 系统介绍

2. 1 编码结构

彩色电视机信号的 PCM 编码有两种方式: 复合信号编码和分量编码。分量编码虽然有许多优越性, 如可根据每一分量带宽降低采样频率, 在进行数字信号处理时排除了副

载波调制带来的麻烦，尤其对于SECAM 制来说，由于色差信号对副载波的调制方式是调频，难于采用复合信号编码，只能采用分量编码方式。但是由于它增加了A/D 数目及解码电路，增加了成本，且经过模拟的编码器会使图像质量有一些损伤，这对于电视广播的解扰系统来说就不太适用，因此我们采用复合信号编码。如图1所示。

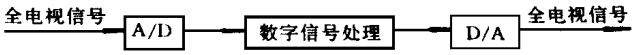

图1　复合信号编码

2.2　量化精度

量化就是把采样值的变化范围分成若干等级，每一级由一个数字表示。因此量化必然带来误差。量化误差在图像中表现为量化杂波（量化噪声），它使得数字化后再生的图像质量下降。显然，量化分级越密，即所用码位越多，量化误差越小，再生图像质量越高。理论分析表明，当量化分级是均匀分布时，信杂比与所用码位N 的关系是

$$S/N = 10.8 + 6 \times N(dB)$$

由此可见每增加一比特可提高信噪比6dB.

在保证图像质量不明显下降的前提下，对电视图像信号量化为8bit 抽样，以避免过高的系统设备成本。

2.3　采样频率

为了防止采样中出现的混叠噪声，根据奈奎斯特定理，采样频率$f_s \geq 2f_m$。但是对于全电视信号而言，它不仅包括亮度信号，还包括与亮度信号频分复用的调制色差信号的彩色付载波。由于量化器是非线性电路，因此将产生抽样频率f_s 与彩色付载波f_{sc} 之间的差拍干扰。对于PAL 信号，为减小拍频与亮度信号的互调制噪声，应使拍频与行频或$1/4f_h$ 间置。由于在PAL 信号中，f_{sc} 与行频或$1/4f_h$ 间置，所以有

$$f_s = (N + 1)f_{sc}$$

因此，取$3f_{sc}$ 或$4f_{sc}$ 都可降低量化的拍频干扰。取$3f_{sc}$ 时比$4f_{sc}$ 时对器件的速度要求和传输、存储要求低得多。但因为PAL 全电视信号与行频是$1/4f_h$ 偏置的，且有25Hz 偏移，所以$f_s = 3f_{sc}$ 的取样结构极其复杂，场间与行间的样点均不垂直对准。因此使祯间处理、场间处理和行间处理均不方便。所以我们采用了$4f_{sc}$ 的采样频率。

$$f_s = 4f_{sc} \approx 4 \times 4.43 \approx 17.72MHz$$

2.4　加扰方式

采用模拟线传输的数字加扰方式，即时基处理方式。具体采用行旋转方式，存储容量小，价格便宜，行旋转加扰过程如图2所示。切割点的位置是用PN 信号序列随机指定。另外，通过限制切割点的位置，就能控制加扰图像的可见度。当采用这种方式时，通过加扰画面可略知节目内容，能起到增加合同用户的作用。PN 信号可每场变一次也可每行变一次。

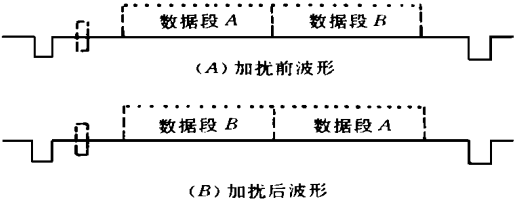

图2　行旋转加扰过程

对于伴音系统不进行加密。这是因为没有图像的伴音能够提起用户的兴趣, 也能增加合同用户。

2.5 存储器容量

采用行旋转方式只需存储2行数据, 每行的容量

$$m = 64\mu s \times 17.7MHz \approx 1133(bit)$$

即一行存储需2K 的芯片, 2行为4K, 每点为8bit. 因此, 总容量为4K ×8 (bit).

2.6 密钥及收费管理

2.6.1 PN 的产生

在数据保密性要求不过高的情况下, 采用了一个9级线性反馈移位寄存器产生 PN 信号。其反馈函数

$$F(X) = X9 \oplus X4$$

其结构如图3.

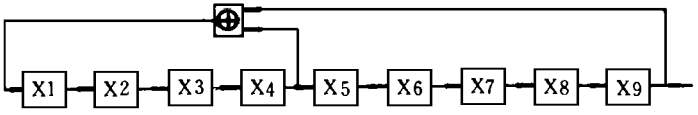

图3 PN 信号的产生

X1…X9作为输出, 因此其产生的数值范围为0～511。

2.6.2 密钥的传输

本系统密钥的传输包括用户设备号及相关信息, PN 系列等数据的传输, 采用的是在行消隐期间 (HBI) 传送的办法。利用17.7MHz 采样频率在一行64μs 期间进行采样, 共有1133个采样点。

从0～146为同步头、行消隐期及色同步信号, 146～186为HBI 期间, 186～1107为视频数据区, 1107～1133也是 HBI 区。

数据的传输在146～186之间进行。为了同步的需要及减少误码, 我们将数据传输频率降低了3倍, 则在146～186期间完成了10bit 的传输。这10bit 的数据分配如下:

X0	X1	X2	X3	X4	X5	X6	X7	X8	X9

X9= 0 PN 信号 X0～X8构成 PN 系列

X9= 1 用户信息 X0～X7用户设备号, 可寻址256个, 必要时可扩展。

X8解扰控制信息, X8= 1允许解扰 X8= 0停止解扰用户信息与PN 不断循环输出, 即可有效控制每个解扰器。

2.7 加扰解扰过程

加扰部分主要包括: A/D, D/A, 存储体, 地址产生器, 时序控制等几部分, 存储体分为 A、B 两部分。地址产生器也分为A、B 两套, 两套相互独立。A 组写入时, B 组读出;

B 组写入时，A 组读出。加扰可在读出时加扰，也可在写入时加扰。

写入加扰过程如下：

(1) 在1133个采样点中，0～186点顺序写入存储体。

(2) 当计数器计到187时，把PN 打入计数器，使图像起点从 PN 开始。

(3) 计数器从 PN 开始计，当计到1107时，存储体已写满，此时再把188打入计数器，把剩余的视频数据写到前面。

(4) 当计数器计到 PN 时，则一行扰乱完成。把1108打入计数器，计到1133该行结束为止。

经以上四步，写入图像体的数据已前后颠倒，从而完成加扰。

解扰过程是加扰的逆过程。

(1) 0～186期间，数据正常读出。

(2) 当计数器计到187时，把 PN 值打入计数器，数据从 PN 开始读出，这时刚好是图像的开始。

(3) 当计数器计到1107时，把187打入计数器，使图像接着放出。

(4) 当计数器计到 PN 时，把1107打入计数器，从而完成行的读出。

以上简单介绍了一种目前比较实用的 CATV 加密管理系统的系统构成及工作方法。

参 考 文 献

1 陈夏娜，杨玉泉，陈欢. 有线电视加扰技术. 北京：广播电影电视部科技情报研究所，1993

2 俞斯乐，郭富云. 电视原理. 北京：国防工业出版社，1985

3 肖国镇，梁传甲，王育民. 伪随机序列及其应用. 北京：国防工业出版社，1985

(责任编辑　卢天贶)