(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1937759 B
(45)授权公告日 2010.08.11

(21)申请号 200510100916.5

(22)申请日 2005.10.31

(73)专利权人 康佳集团股份有限公司
地址 518053 广东省深圳市南山区华侨城康佳集团

(72)发明人 陶显芳

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 高占元

(51)Int.Cl.
H04N 7/16(2006.01)

(56)对比文件
CN 1406067 A,2003.03.26, 全文.
CN 1633069 A,2005.06.29, 全文.
CN 1522069 A,2004.08.18, 全文.
CN 1210423 A,1999.03.10, 说明书10页第7行至第22行.
WO 200471091 A1,2004.08.19, 说明书第3页第10行至第29行.

审查员 王博

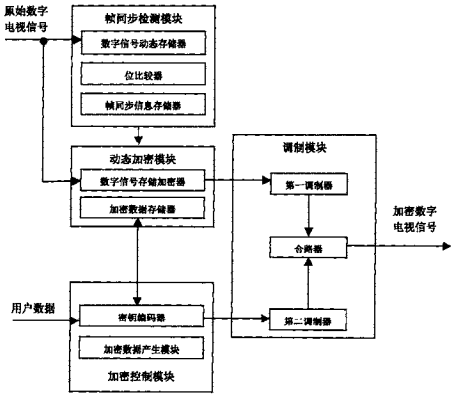
权利要求书 1 页 说明书 4 页 附图 2 页

(54)发明名称

一种随路密钥数字电视信号加密系统

(57)摘要

本发明公开了一种随路密钥数字电视信号加密系统,包括发送端对原始数字电视信号进行加密,和对用户数据的管理,以及加密数字电视信号和数据信号的传送;接收端,通过对数据信息进行处理,用密钥对加密数字电视信号进行解密。对数字电视信号进行加密的方法,主要是通过对数字电视信号进行动态存储,然后与原数字电视信号的数据进行位比较,检测出数字信号的同步头和结束码,再用新的同步头数据置换原始数字信号的同步头。具体包括:A1)用移位存储器对原始数字电视信号的数据进行动态存储;A2)用位比较器对原始数字电视信号进行帧检测;A3)用加密数据作为新的数字电视信号的同步头和结束码,置换原始数字电视信号中的同步头和结束码。



CN 1937759 B

1. 一种随路密钥数字电视信号加密系统，将原始数字电视信号转换为加密数字电视信号，其特征在于，包括：

与所述原始数字电视信号相连，用于对所述原始数字电视信号的帧同步信息进行检测并输出同步触发信号的帧同步检测模块；所述帧同步检测模块包括，用于存储原始数字电视信号的数字信号动态存储器，用于存储原始数字电视信号帧同步比特的帧同步信息存储器；还包括和所述帧同步信息存储器和所述数字信号动态存储器相连，并对所述帧同步信息存储器的数据和所述数字信号动态存储器的数据进行按位比较，并在所述数字信号动态存储器的帧同步位置的比特和所述帧同步信息存储器的同步比特完全一致时产生同步触发信号的位比较器；

用于同时产生加密数据和对应密钥的加密控制模块；

与所述原始数字电视信号、所述帧同步检测模块和所述加密控制模块相连，在所述同步触发信号控制下，利用移位寄存器和位比较器实现所述加密数据对原始数字电视信号进行加密，产生帧加密的数字电视信号的动态加密模块；

与所述加密控制模块和所述动态加密模块相连，将所述帧加密的数字电视信号和所述密钥合并，并转换为适合传输的加密数字电视信号的调制模块。

2. 根据权利要求 1 所述随路密钥数字电视信号加密系统，其特征在于，所述动态加密模块包括存储用于替换原始数字电视信号帧同步比特的加密同步比特的加密数据存储器，和所述原始数字电视信号相连，动态存储原始数字电视信号，并在所述同步触发信号有效时，使用所述加密同步比特替换原始数字电视信号中的帧同步比特，产生所述帧加密的数字电视信号的数字信号存储加密器。

3. 根据权利要求 2 所述随路密钥数字电视信号加密系统，其特征在于，所述加密控制模块包括用于产生加密数据和对应密钥的加密数据产生模块；用于对所述密钥进行编码产生密钥比特的密钥编码器。

4. 根据权利要求 3 所述随路密钥数字电视信号加密系统，其特征在于，所述加密数据和密钥随时间变化。

5. 根据权利要求 3 所述随路密钥数字电视信号加密系统，其特征在于，所述密钥编码器还可以接收用户数据，并将密钥和用户数据同时进行编码产生所述密钥比特。

6. 根据权利要求 3 所述随路密钥数字电视信号加密系统，其特征在于，所述调制模块包括用于对所述帧加密的数字电视信号进行调制的第一调制器；用于对所述密钥比特进行调制的第二调制器；用于将所述第一调制器和所述第二调制器输出的信号进行合路产生可以用于传输的加密数字电视信号的合路器。

7. 根据权利要求 6 所述随路密钥数字电视信号加密系统，其特征在于，所述第一调制器为数字调制器。

8. 根据权利要求 6 所述随路密钥数字电视信号加密系统，其特征在于，所述第二调制器为模拟调制器。

一种随路密钥数字电视信号加密系统

技术领域

[0001] 本发明涉及数字电视系统，特别涉及数字电视系统加密系统。

背景技术

[0002] 目前我国的数字电视节目正准备开始广播，数字电视取代模拟电视机已是指日可待，但困扰我国数字电视发展的节目信号加密，和有条件接收的技术问题，一直没有很好解决。

[0003] 数字电视信号以数据帧的形式进行传输，传输的码率很高，特别是高清晰度数字电视 (HDTV)，码率高达 20MPS 以上，因此信号的加密解密一般都需要用含有 DSP 功能的 RISC-CPU(如 :ARM-CPU) 或 SOC 等高速数据处理器件或电路来实现。使用这些器件还需要嵌入式操作系统软件，和中间件及数据处理软件来支持。因此，硬件成本很高，软件开发难度也很大。

[0004] 因此，针对以上对数字电视节目信号加密和解密方法成本高，技术开发难度大等缺点，有必要开发一种简单易行、低成本的数字电视系统节目加密系统和方法。

发明内容

[0005] 本发明所要解决的技术问题是提供一种简单易行、低成本的随路密钥的数字电视信号加密系统。

[0006] 本发明解决问题的技术方案是，构造一种随路密钥数字电视信号加密系统，将原始数字电视信号转换为加密数字电视信号，包括与所述原始数字电视信号相连，用于对所述原始数字电视信号进行帧信息检测划分并输出同步触发信号的帧同步检测模块 ；用于同时产生加密数据和对应密钥的加密控制模块 ；

[0007] 与所述原始数字电视信号、所述帧同步检测模块和所述加密控制模块相连，在所述同步触发信号控制下，利用所述加密数据对原始数字电视信号进行加密产生帧加密的数字电视信号的动态加密模块 ；利用移位寄存器和判断单元实现所述加密数据对原始数字电视信号进行加密，产生帧加密的数字电视信号的动态加密模块 ；

[0008] 与所述加密控制模块和所述动态加密模块相连，将所述帧加密的数字电视信号和所述密钥合并，并转换为适合传输的加密数字电视信号的调制模块。

[0009] 帧同步检测模块包括，用于存储原始数字电视信号的数字信号动态存储器，用于存储原始数字电视信号帧同步比特的帧同步信息存储器，还包括和所述帧同步信息存储器和所述数字信号动态存储器相连，并对所述帧同步信息存储器的数据和所述数字信号动态存储器的数据进行按位比较，并在所述数字信号动态存储器的帧同步位置的比特和所述帧同步信息存储器的同步比特完全一致时产生同步触发信号的位比较器。

[0010] 动态加密模块包括存储用于替换原始数字电视信号帧同步比特的加密同步比特的加密数据存储器，和所述原始数字电视信号相连，动态存储原始数字电视信号，并在所述同步触发信号有效时，使用所述加密同步比特替换原始数字电视信号中的帧同步比特产生

所述帧加密的数字电视信号的数字信号存储加密器。

[0011] 加密控制模块包括用于产生加密数据和对应密钥的加密数据产生模块；用于对所述密钥进行编码产生密钥比特的密钥编码器。加密数据产生的加密数据和密钥可为随路信号，即随时间变化，以提高加密系统的安全性。所述密钥编码器还可以接收用户数据，并将密钥和用户数据同时进行编码。

[0012] 调制模块包括用于对所述帧加密的数字电视信号进行调制的第一调制器；用于对所述密钥比特进行调制的第二调制器；用于将所述第一调制器和所述第二调制器输出的信号进行合路产生可以用于传输的加密数字电视信号的合路器。其中第一调制器为数字调制器，第二调制器为模拟调制器。

[0013] 加密后的数字电视信号和密钥一起传送到接收端，接收端通过利用密钥对加密数字电视信号进行解密，还原出原始的数字电视信号。

[0014] 采用本发明的方法，关键是对数据比特进行帧的划分，只需要设计一些移位寄存器和逻辑判断单元即可实现，因此可以使用可编程逻辑器件如 CPLD/EPLD/FPGA 实现，电路简单、成本低。而且加密解密不需要软件开发，更不需要操作系统平台，因而技术开发难度低，可靠性也可以进一步提高。

[0015] 以下结合附图通过实施列对本发明做进一步详细说明。

附图说明

[0016] 图 1 所示为数字电视信号在传输过程中的基本编码格式；

[0017] 图 2 所示为本发明的随路密钥数字电视信号加密系统的原理框图；

[0018] 图 3 所示为根据本发明的随路密钥数字电视信号加密系统的一种优选实施方式的原理框图；

[0019] 图 4 所示为根据本发明的随路密钥数字电视信号加密系统的一种优选实施方式调制频谱图。

具体实施方式

[0020] 图 1 是数字电视信号在传输过程中的基本编码格式，也是一般数字信号的基本传送编码格式。在这种编码格式中包括同步头，传送数据，和结束码等三个主要组成部分，同步头和结束码统称为帧同步码，或同步比特。这种数据结构，人们都把它称为“帧”，数字信号就是一帧一帧地传送的。同步头和结束码分别都由若干比特来组成，一般帧的比特数越多，即帧的长度越长，且两相邻帧之间的间隔越短，则要求同步头和结束码的比特位数也越多。如果两相邻帧之间的间隔非常长，则同步头和结束码只需要一个或两个比特即可足够。帧的长短主要由数据内容来决定，帧与帧的间隔则由数据传送量来决定。数字电视信号的信息量很大，因此帧取得很长，间隔也很短。

[0021] 在数字信号传输过程中，如果失去了同步头和结束码，或把同步头和结束码弄错，信号就无法传送数据，因为这相当于使信号失去了时序，没有时序就无法从信号中把数据进行分离和解码。

[0022] 如图 2 所示为本发明的随路密钥数字电视信号加密系统的原理框图。通过随路密钥数字电视信号加密系统，将原始数字电视信号转换为加密数字电视信号。对数字电视信

号进行加密主要是通过对数字电视信号进行动态存储，然后对原数字电视信号的数据进行位比较，检测出数字信号的同步比特，再用新的同步比特置换原始数字信号的同步头。

[0023] 随路密钥数字电视信号加密系统包括与原始数字电视信号相连，用于对原始数字电视信号进行帧信息检测并输出同步触发信号的帧同步检测模块；用于同时产生加密数据和对应密钥的加密控制模块；

[0024] 与原始数字电视信号、帧同步检测模块和加密控制模块相连，在同步触发信号控制下，利用加密数据对原始数字电视信号进行加密产生帧加密的数字电视信号的动态加密模块；

[0025] 与加密控制模块和动态加密模块相连，将帧加密的数字电视信号和密钥合并，并转换为适合传输的加密数字电视信号的调制模块。

[0026] 帧同步检测模块包括，用于存储原始数字电视信号的数字信号动态存储器，用于存储原始数字电视信号帧同步比特的帧同步信息存储器，还包括和帧同步信息存储器和数字信号动态存储器相连，并对帧同步信息存储器的数据和数字信号动态存储器的数据进行按位比较，并在数字信号动态存储器的帧同步位置的比特和帧同步信息存储器的同步比特完全一致时产生同步触发信号的位比较器。

[0027] 动态加密模块包括存储用于替换原始数字电视信号帧同步比特的加密同步比特的加密数据存储器，和原始数字电视信号相连，动态存储原始数字电视信号，并在同步触发信号有效时，使用加密同步比特替换原始数字电视信号中的帧同步比特产生所述帧加密的数字电视信号的数字信号存储加密器。

[0028] 加密控制模块包括用于产生加密数据和对应密钥的加密数据产生模块；用于对所述密钥进行编码产生密钥比特的密钥编码器。加密数据和密钥可以设计为随时间变化。密钥编码器还可以接收用户数据，并将密钥和用户数据同时进行编码。

[0029] 调制模块包括用于对帧加密的数字电视信号进行调制的第一调制器；用于对密钥比特进行调制的第二调制器；用于将第一调制器和第二调制器输出的信号进行合路产生可以用于传输的加密数字电视信号的合路器。其中第一调制器为数字调制器，第二调制器为模拟调制器。

[0030] 如图 4 所示为根据本发明的随路密钥数字电视信号加密系统的一种优选实施方式的原理框图。

[0031] 原始数字电视信号被输入加密系统时，被分成两路信号，一路用于对原始数字电视信号的帧数据或帧同步信号进行检测，另一路用于对数字电视信号进行加密和加密信号输出。

[0032] 移位寄存器 1 构成数字信号动态存储器，移位寄存器 2 构成数字信号存储加密器。帧同步信息存储器具体为存储器 1，加密数据存储器具体为存储器 2。

[0033] 存储器 1 由电脑通过数据接口电路写入原始数字电视信号中的一些基本数据，如：同步头，结束码，以及其它一些不会经常变化的数据，这些基本数据也可以称为数字电视信号的特征码。存储器 1 中的数据被作为位比较器的其中一路输入数据，位比较器的另一路输入数据来自移位寄存器 1 的并联输出。移位寄存器 1 的数据被一位一位地输入，以及一位一位地被存储，移位寄存器 1 存储器的数据可以一次全部输出（并联输出），或把一位一位地从输出口输出（串联输出）。

[0034] 位比较器时刻监测移位寄存器 1 中的数据和存储器 1 中的数据比特是否一致，当两者一致时，即移位寄存器 1 中刚好位完成的一帧数据时，位比较器输出一个触发信号给存储器 2，让存储器 2 中的存储的加密的同步头和结束码信息替换移位寄存器 2 中的原有的帧中同步头和结束码。

[0035] 加密数据和密钥由电脑产生，加密数据通过数据写入接口写入存储器 2，在没有同步触发信号到来之前，移位寄存器 2 存储的数据与移位寄存器 1 存储的数据完全相同。当加密同步信号到来时，控制信号就会把存储器 2 中存储的加密数据读出，送给移位寄存器 2 进行存储，即把一帧原始数字电视信号的帧同步头和结束码用加密数据替换，然后以串联的方式，把数据一位一位地从移位寄存器 2 中输出。

[0036] 移位寄存器 1 和移位寄存器 2 都连接到开关 K，分别输出未经加密和加密的数字电视信号帧数据。经过开关 K 选择可以选择输出未经加密或加密的数字电视信号帧数据。

[0037] 调制器 1 为第一调制器，完成数字电视信号的数字调制，产生为数字电视基带信号然后再经过高频调制，把基带信号调制成为数字电视高频信号，最后就可以通过有线电视信号传送系统、高频发射天线，或卫星广播系统进行传输。

[0038] 调制器 2 为第二调制器，密钥的传输与加密数字电视信号共用一个高频传送系统，但密钥经编码后，不是进行数字调制，而是采用调制器 2 进行模拟调制，经模拟调制后的密钥比特信号，同样也要进行高频调制，经高频调制后的用户数据以及密钥比特高频信号再与数字电视高频信号混合，就可以一起在同一系统中传输。

[0039] 目前我国 PAL 彩色电视制式标准中，视频带宽为 6 兆，伴音带宽为 500KHz，采用以上加密方法，6 兆带宽仍然可以用于加密数字电视信号传输，如采用 QAM64 数字调制，最高码率可达 36MPS，而密钥比特则可采用模拟调制。若数据信号选用调制频率为 6.5MHz 载波来进行 ASK（键控调幅）或 FSK（键控调频）调制（双边带），则码率最高可达 500KPS。这完全能够满足数字有线电视节目加密信号的传输要求，两个载波频率的频谱分布如图 4 所示。f_D 为数据高频调制信号（二次调制）的中心频率，它一般位于频道带宽的边缘，f_P 为数字音视频编码信号高频载波（二次调制）的中心频率（电视频道频率）。实际上完全实现单边带发送在技术上是很困难的，因此图 4 表示的是一个残留边带频谱分布图。

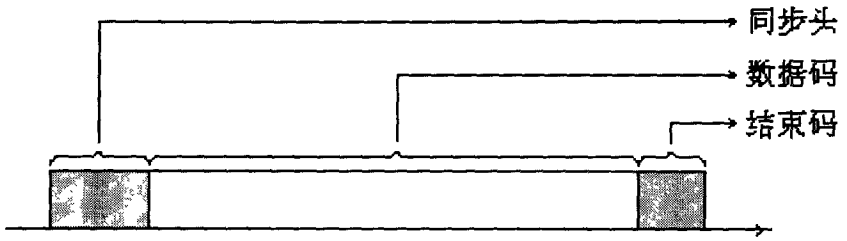

同步头
数据码
结束码

图 1

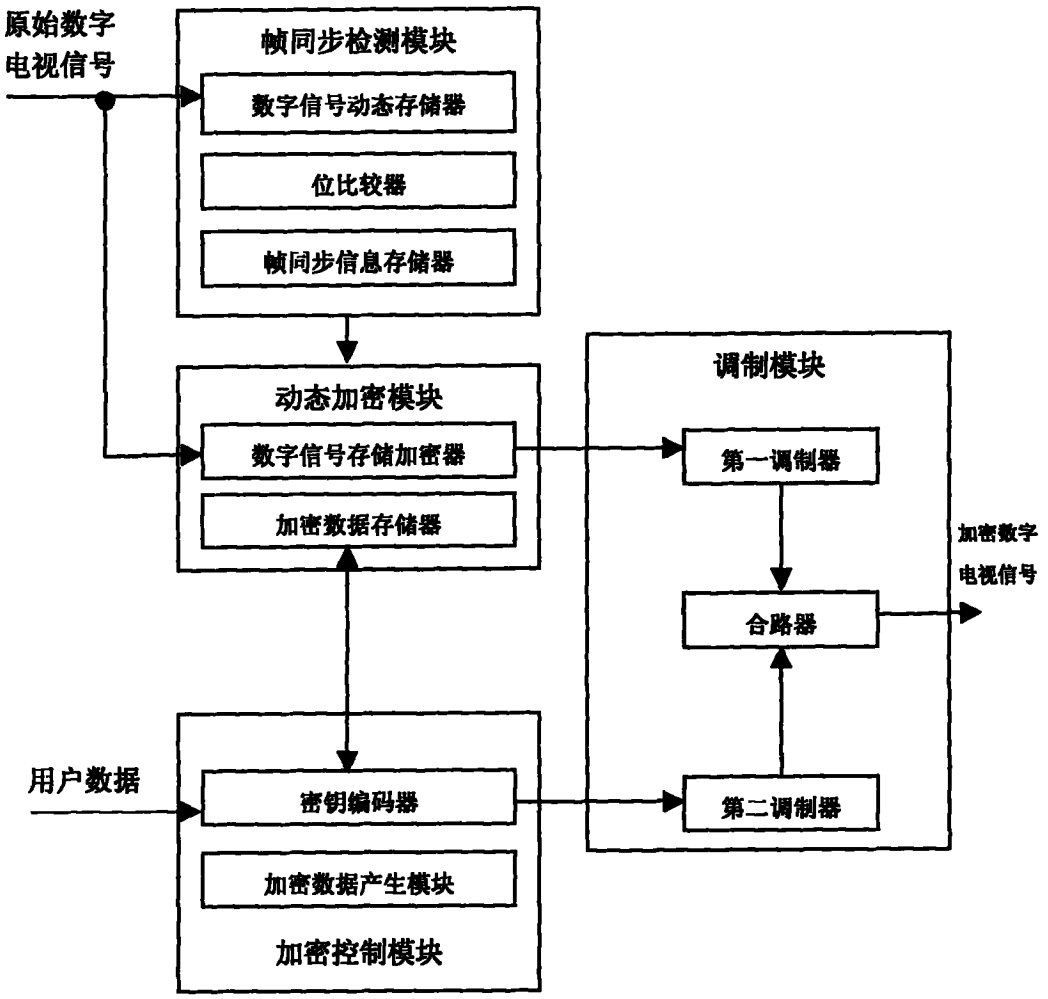

原始数字
电视信号
帧同步检测模块
数字信号动态存储器
位比较器
帧同步信息存储器
动态加密模块
数字信号存储加密器
加密数据存储器
调制模块
第一调制器
合路器
加密数字
电视信号
用户数据
密钥编码器
加密数据产生模块
加密控制模块
第二调制器

图 2

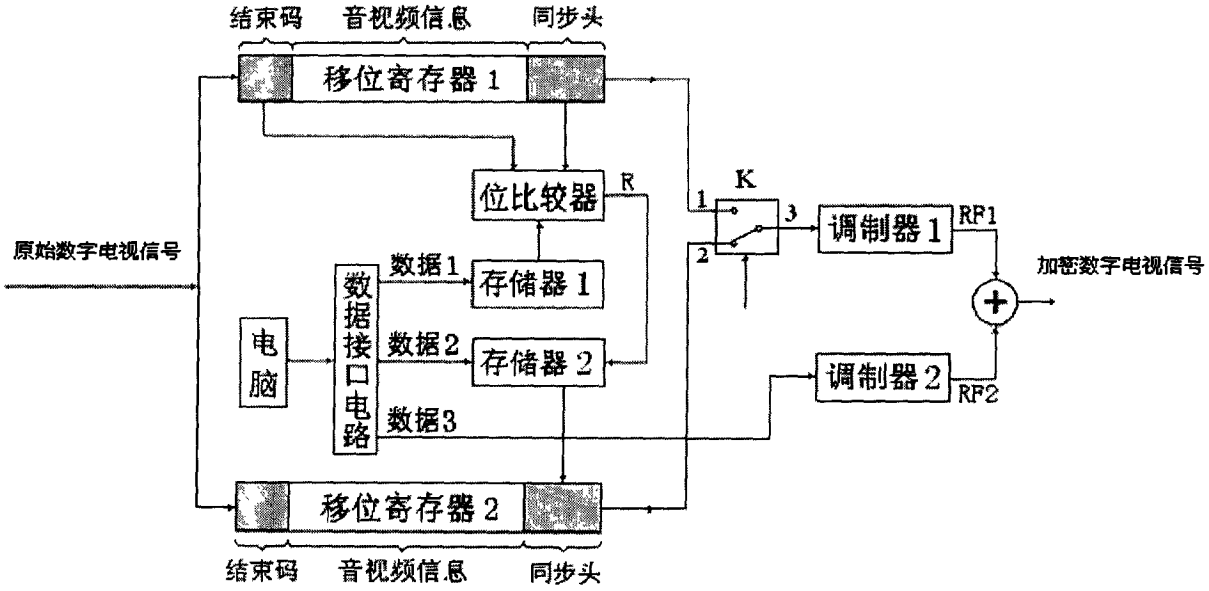

结束码
音视频信息
同步头
移位寄存器 1
位比较器
R
K
1
2
3
调制器 1
RF1
原始数字电视信号
数据1
存储器 1
数据接口电路
电脑
数据2
存储器 2
数据3
调制器 2
RF2
加密数字电视信号
移位寄存器 2
结束码
音视频信息
同步头

图 3

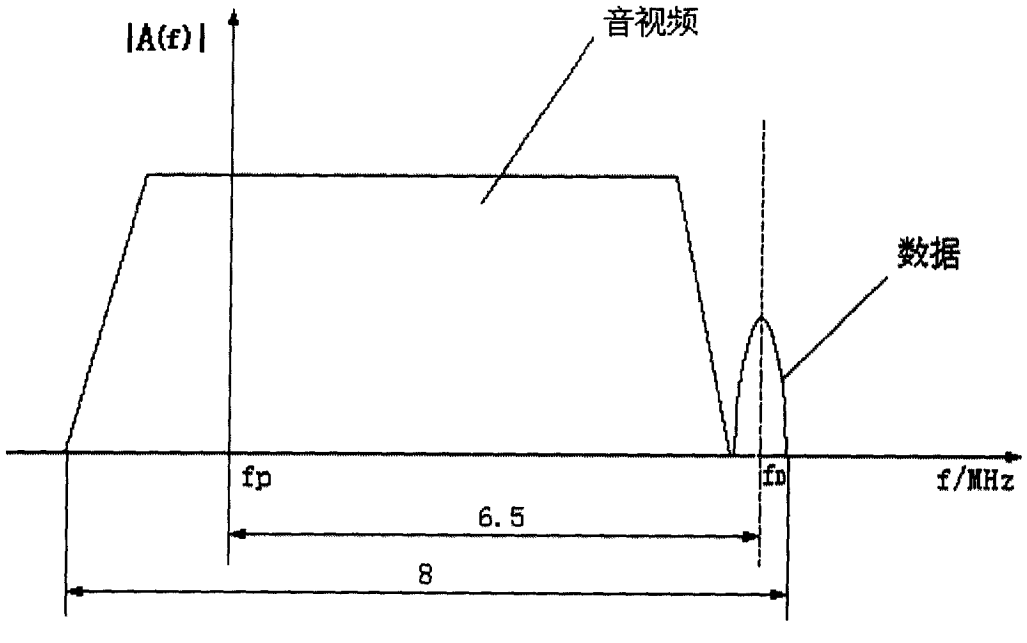

|A(f)|
音视频
数据
fp
fD
f/MHz
6.5
8

图 4