(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 102857832 A
(43)申请公布日 2013.01.02

(21)申请号 201210379166.X

(22)申请日 2012.10.09

(71)申请人 安徽天虹数码技术有限公司
地址 230031 安徽省合肥市井岗路68号蜀山自主创新产业基地7幢8F

(72)发明人 李勇 张进 王满海 廖亮亮 吴冬明 许亚兰

(74)专利代理机构 合肥天明专利事务所 34115
代理人 吴娜

(51)Int.Cl.
H04N 21/8358(2011.01)
H04N 5/913(2006.01)

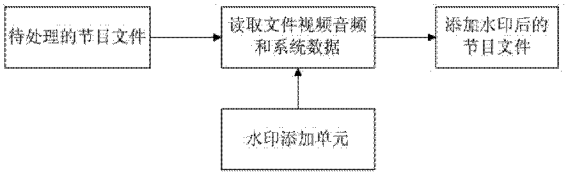
权利要求书 1 页 说明书 2 页 附图 2 页

(54)发明名称

防恶意操作硬盘播出系统节目文件的保护方法及系统

(57)摘要

本发明涉及一种防恶意操作硬盘播出系统节目文件的保护方法，包括：水印添加单元对通过审查的节目文件添加水印；在节目文件播出前，水印检测单元打开已经添加过水印的节目文件，并检测其水印是否正常，若检测结果为是，则播出该节目文件，否则，停止检测并报警。本发明还公开了一种防恶意操作硬盘播出系统节目文件的保护系统。本发明通过水印添加单元对经过上载后的节目文件添加水印标记，如果节目文件被非法替换或修改，那么节目文件中的水印必然被破坏，因此，在节目文件播出前，可通过水印检测单元检测其水印，如果节目文件中没有水印、水印不正确或不完整，即意味着节目文件被替换或修改，系统可发出告警，提醒及时处理。



CN 102857832 A

1. 一种防恶意操作硬盘播出系统节目文件的保护方法，该方法包括下列顺序的步骤：

（1）水印添加单元对通过审查的节目文件添加水印；

（2）在节目文件播出前，水印检测单元打开已经添加过水印的节目文件，并检测其水印是否正常，若检测结果为是，则播出该节目文件，否则，停止检测并报警。

2. 根据权利要求 1 所述的防恶意操作硬盘播出系统节目文件的保护方法，其特征在于：在添加水印之前，由上载单元打开通过审查的节目文件，并依次读取该节目文件的视频、音帧频和系统数据，

再由水印添加单元对所读取的视频、音帧频和系统数据添加水印。

3. 根据权利要求 1 所述的防恶意操作硬盘播出系统节目文件的保护方法，其特征在于：所述的水印检测单元在检测节目文件的水印正常之后，由播出单元播出该节目文件。

4. 根据权利要求 1 所述的防恶意操作硬盘播出系统节目文件的保护方法，其特征在于：水印添加单元对节目文件进行水印添加的方式由用户设定；水印检测单元进行水印检测的方式与水印添加的方式相对应。

5. 根据权利要求 1 所述的防恶意操作硬盘播出系统节目文件的保护方法，其特征在于：在节目文件播出前，水印检测单元打开已经添加过水印的节目文件，如果无法找到该节目文件，则立即报警。

6. 根据权利要求 1 所述的防恶意操作硬盘播出系统节目文件的保护系统，其特征在于：包括用于对通过审查的节目文件添加水印的水印添加单元，其输出端与用于检测节目文件水印的水印检测单元的输入端相连，水印检测单元的输出端分别与用于播出节目文件的播出单元、报警单元的输入端相连。

7. 根据权利要求 6 所述的防恶意操作硬盘播出系统节目文件的保护系统，其特征在于：还包括上载单元，其输出端与水印添加单元的输入端相连。

防恶意操作硬盘播出系统节目文件的保护方法及系统

技术领域

[0001] 本发明涉及电视广播领域，尤其是一种防恶意操作硬盘播出系统节目文件的保护方法及系统。

背景技术

[0002] 目前，电视硬盘播出系统对于硬件故障、软件故障、病毒攻击、网络中断、电源故障等安全隐患，具有较好的安全防护措施，但是对于电视台内部工作人员，例如播出操作人员的恶意播出非法节目的操作却缺乏防护。2012 年 7 月 7 日 19 :20 分，重庆酉阳资讯电视台播放了超过 3 分钟的淫秽影片，事后查明犯罪嫌疑人杨某系酉阳县电视台正式职工，因对单位管理不满，事先将电视节目恶意篡改， 植入境外淫秽影片片段。可见，硬盘播出系统对各种可能的技术故障都具备了较为完善的安全措施，但是对于电视台内部操作人员出于种种原因，将正常节目文件替换、修改为非法节目内容并进而播出，以达到某种政治目的或其它非法目的这一可能现象，缺乏相应的安全防范措施。

发明内容

[0003] 本发明的首要目的在于提供一种通过对待保护的节目文件添加水印，实现对节目文件的保护的防恶意操作硬盘播出系统节目文件的保护方法，该方法包括下列顺序的步骤：

（1）水印添加单元对通过审查的节目文件添加水印；

（2）在节目文件播出前，水印检测单元打开已经添加过水印的节目文件，并检测其水印是否正常，若检测结果为是，则播出该节目文件，否则，停止检测并报警。

[0004] 本发明还公开了一种防恶意操作硬盘播出系统节目文件的保护系统，包括用于对通过审查的节目文件添加水印的水印添加单元，其输出端与用于检测节目文件水印的水印检测单元的输入端相连，水印检测单元的输出端分别与用于播出节目文件的播出单元、报警单元的输入端相连。

[0005] 由上述技术方案可知，本发明通过水印添加单元对经过上载后的节目文件添加水印标记，如果节目文件被非法替换或修改，那么节目文件中的水印必然被破坏，因此，在节目文件播出前，可通过水印检测单元检测其水印，如果节目文件中没有水印、水印不正确或不完整，即意味着节目文件被替换或修改，系统可发出告警，提醒及时处理。

附图说明

[0006] 图 1 为本发明中水印添加单元的工作流程图；

图 2 为本发明中水印检测单元的工作流程图；

图 3 为本发明的系统结构框图。

具体实施方式

[0007] 一种防恶意操作硬盘播出系统节目文件的保护方法，该方法包括下列顺序的步骤：(1)水印添加单元对通过审查的节目文件添加水印；(2)在节目文件播出前，水印检测单元打开已经添加过水印的节目文件，并检测其水印是否正常，若检测结果为是，则证明节目文件没有被修改和替换，播出该节目文件，否则，停止检测并报警。所述的水印检测单元在检测节目文件的水印正常之后，由播出单元播出该节目文件。如图1、2所示。

[0008] 如图1、2所示，在添加水印之前，由上载单元打开通过审查的节目文件，并依次读取该节目文件的视频、音帧频和系统数据，再由水印添加单元对所读取的视频、音帧频和系统数据添加水印。水印添加单元对节目文件进行水印添加的方式由用户设定；水印检测单元进行水印检测的方式与水印添加的方式相对应。在节目文件播出前，水印检测单元打开已经添加过水印的节目文件，如果无法找到该节目文件，则立即报警。

[0009] 数字水印(Digital Watermarking)技术是将一些标识信息直接嵌入数字载体当中(包括多媒体、文档、软件等)或是间接表示(修改特定区域的结构)，且不影响原载体的使用价值，也不容易被探知和再次修改，但可以被生产方识别和辨认。通过这些隐藏在载体中的信息，可以达到确认内容创建者、购买者、传送隐秘信息或者判断载体是否被篡改等目的。数字水印技术从20世纪90年代初开始兴起，现在已经是一种相当成熟的技术，但同时仍然处于快速发展之中。

[0010] 水印技术牵涉到密码学、视频编解码技术、音频编解码技术等内容，目前有基于离散余弦变换、离散小波变换及其它一些变换域的水印算法，小波数字水印算法是目前的主流。不同的水印添加方式具有不同的稳健性、安全性、计算复杂性，一般来说，安全性高、稳健性好的添加方式，其计算复杂性也大，对系统的硬件性能要求也高，可以根据用户对安全性、稳健性的不同需求层次，结合系统硬件性能选择合适的添加方式。

[0011] 如果节目文件中添加的水印过少，那么在大量的没有添加水印的节目内容处，就可能被替换成恶意内容，因此添加的水印越多，越安全，但是对系统的硬件性能要求也越高。可以根据用户对安全性的需求确定需要添加水印的视频音频帧占全部视音频帧的比例，比例越高，安全性越高，但同时对硬件性能要求也越高。根据用户要求的添加水印的视频音频帧所占比例，确定当前视频音频帧和系统数据是否添加水印，如果需要添加水印，则添加水印，否则跳过。

[0012] 不同的水印添加方式采用不同的算法原理，因此要根据用户设定的水印添加算法选择相应的检测算法，水印检测方式要和水印添加方式一一对应起来，并且根据用户设定的具体参数，例如添加水印的视频音频帧比例，来确定水印检测单元的相应参数。

[0013] 如图3所示，本系统包括用于对通过审查的节目文件添加水印的水印添加单元，其输出端与用于检测节目文件水印的水印检测单元的输入端相连，水印检测单元的输出端分别与用于播出节目文件的播出单元、报警单元的输入端相连。还包括上载单元，其输出端与水印添加单元的输入端相连。

[0014] 综上所述，本发明通过水印添加单元对经过上载后的节目文件添加水印标记，如果节目文件被非法替换或修改，那么节目文件中的水印必然被破坏，因此，在节目文件播出前，可通过水印检测单元检测其水印，如果节目文件中没有水印、水印不正确或不完整，即意味着节目文件被替换或修改，系统可发出告警，提醒及时处理。

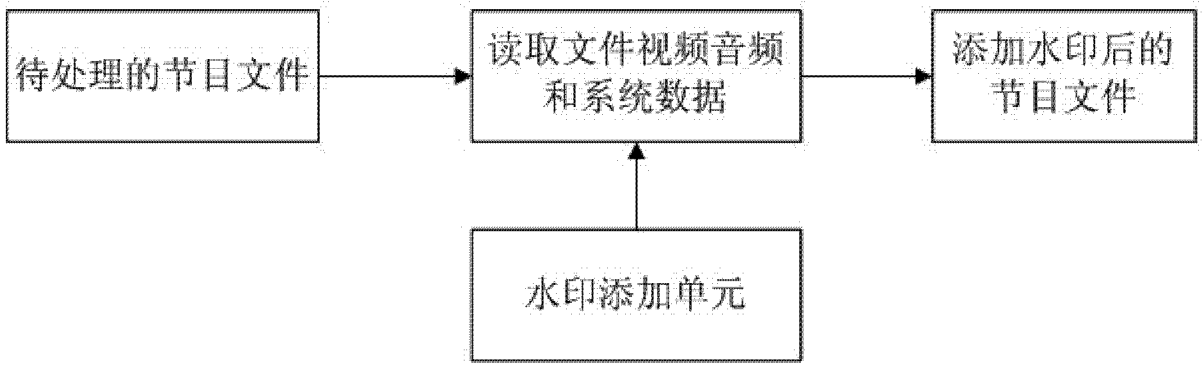

待处理的节目文件
读取文件视频音频和系统数据
添加水印后的节目文件
水印添加单元

图 1

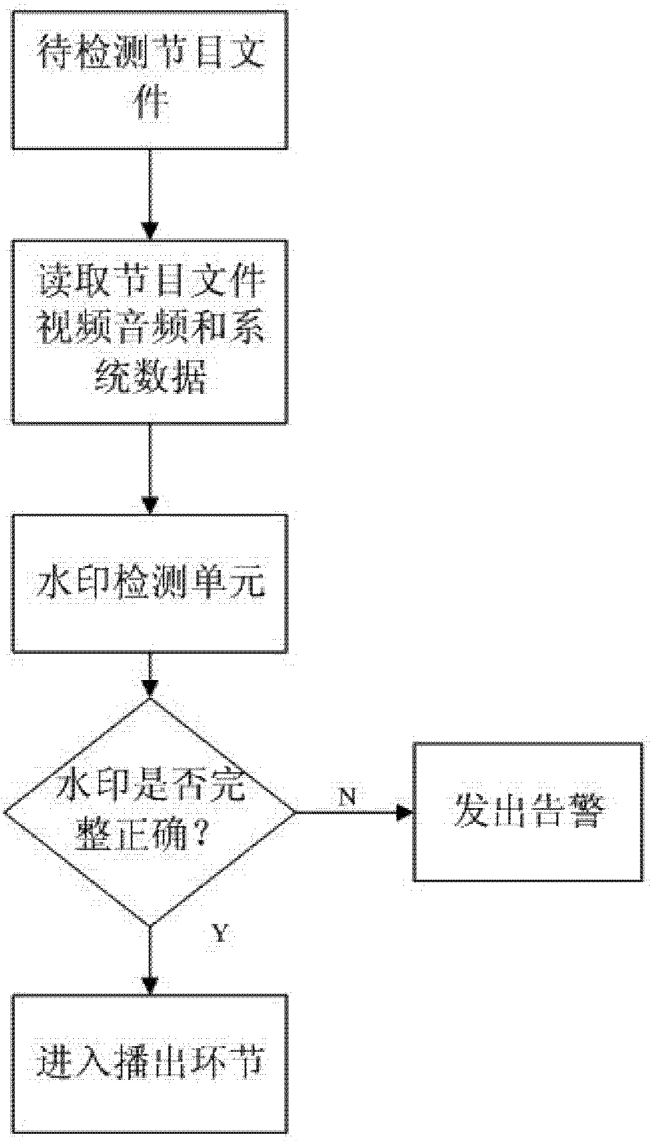

待检测节目文件
读取节目文件视频音频和系统数据
水印检测单元
水印是否完整正确？
N
发出告警
Y
进入播出环节

图 2

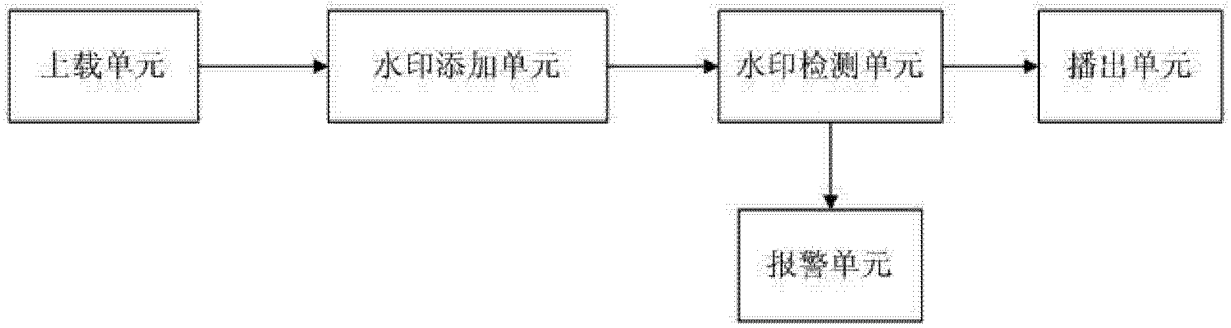


图 3