(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 112054890 B
(45)授权公告日 2024.06.07

(21)申请号 201910493409.4

(22)申请日 2019.06.06

(65)同一申请的已公布的文献号
申请公布号 CN 112054890 A

(43)申请公布日 2020.12.08

(73)专利权人 西安诺瓦星云科技股份有限公司
地址 710075 陕西省西安市高新区丈八街办科技二路72号西安软件园零壹广场DEF101

(72)发明人 张敏 韩丹

(74)专利代理机构 深圳精智联合知识产权代理有限公司 44393
专利代理师 邓铁华

(51)Int.Cl.
H04L 9/06(2006.01)
H04L 9/08(2006.01)
H04L 9/32(2006.01)
H04L 67/30(2022.01)
G06F 21/84(2013.01)
G06F 21/46(2013.01)

(56)对比文件
CN 103139201 A,2013.06.05
CN 106571911 A,2017.04.19
KR 20050077329 A,2005.08.02
KR 20080043217 A,2008.05.16
US 2005005154 A1,2005.01.06
US 6111953 A,2000.08.29
CN 101937501 A,2011.01.05
CN 104217230 A,2014.12.17
CN 103093137 A,2013.05.08
CN 103560879 A,2014.02.05
CN 106034123 A,2016.10.19
CN 108965222 A,2018.12.07
JP 2016075765 A,2016.05.12
US 2015010142 A1,2015.01.08

审查员 白红昌

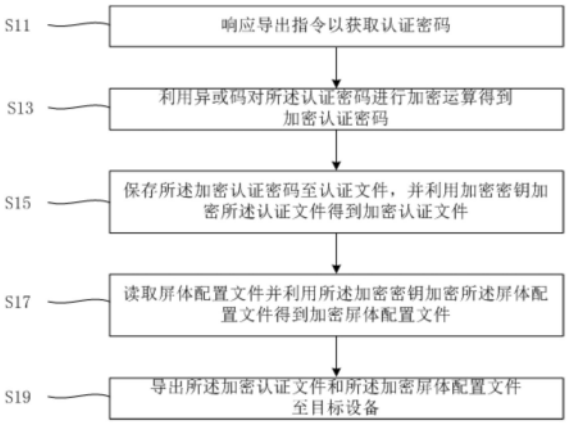
权利要求书2页 说明书8页 附图2页

(54)发明名称

屏体配置文件导出、导入方法及其装置和播控设备

(57)摘要

本发明实施例公开了一种屏体配置文件导出方法及其装置、一种屏体配置文件导入方法及其装置和一种播控设备。所述屏体配置文件导出方法例如包括:响应导出指令以获取认证密码;利用异或码对所述认证密码进行加密运算得到加密认证密码;保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件;读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件;以及导出所述加密认证文件和所述加密屏体配置文件至目标设备。本发明实施例可以提高显示屏播放节目更新的高防护性和高可靠性。



CN 112054890 B

1.一种屏体配置文件导出方法,其特征在于,包括:

响应导出指令以获取认证密码;

利用异或码对所述认证密码进行加密运算得到加密认证密码;

保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件;

读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件;以及

导出所述加密认证文件和所述加密屏体配置文件至目标设备;

其中,所述异或码和所述加密密钥为动态生成。

2.如权利要求1所述的屏体配置文件导出方法,其特征在于,所述屏体配置文件包括屏体总带载大小、单个网口屏体带载数量、屏体走线方式和/或单个屏体大小。

3.如权利要求1所述的屏体配置文件导出方法,其特征在于,所述利用加密密钥加密所述认证文件得到加密认证文件采用的加密方式为DES加密方式,和/或所述利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件采用的加密方式为DES加密方式。

4.如权利要求1所述的屏体配置文件导出方法,其特征在于,在所述导出所述加密认证文件和所述加密屏体配置文件至目标设备之后,所述屏体配置文件导出方法还包括:

发送所述异或码和所述加密密钥以供播控设备获取;其中所述目标设备为用于向所述播控设备导入所述加密认证文件和所述加密屏体配置文件的移动存储设备,或者所述目标设备为所述播控设备。

5.一种屏体配置文件导出装置,其特征在于,包括:

认证密码获取模块,用于响应导出指令以获取认证密码;

认证密码加密模块,用于利用异或码对所述认证密码进行加密运算得到加密认证密码;

认证文件加密模块,用于保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件;

屏体配置文件加密模块,用于读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件;以及

文件导出模块,用于导出所述加密认证文件和所述加密屏体配置文件至目标设备;

其中,所述异或码和所述加密密钥为动态生成。

6.如权利要求5所述的屏体配置文件导出装置,其特征在于,所述屏体配置文件包括屏体总带载大小、单个网口带载屏体数量、屏体走线方式和/或单个屏体大小。

7.如权利要求5所述的屏体配置文件导出装置,其特征在于,所述认证文件加密模块具体用于利用所述加密密钥并采用DES加密方式加密所述认证文件得到所述加密认证文件,和/或所述屏体配置文件加密模块具体用于利用所述加密密钥并采用DES加密方式加密所述屏体配置文件得到所述加密屏体配置文件。

8.如权利要求5所述的屏体配置文件导出装置,其特征在于,所述屏体配置文件导出装置还包括:

密码发送模块,用于发送所述异或码和所述加密密钥以供播控设备获取;其中所述目标设备为用于向所述播控设备导入所述加密认证文件和所述加密屏体配置文件的移动存

储设备,或者所述目标设备为所述播控设备。

9.一种屏体配置文件导入方法,其特征在于,执行于播控设备,包括:

响应导入指令以读取目标设备上的加密认证文件;

利用解密密钥解密所述加密认证文件得到认证文件;

读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码得到认证密码;以及

当所述认证密码与所述播控设备接收或存储的认证密码一致时,读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件,得到屏体配置文件以用于屏体配置;

其中,所述异或码和所述解密密钥为动态生成。

10.如权利要求9所述的屏体配置文件导入方法,其特征在于,所述利用解密密钥解密所述加密认证文件得到认证文件采用的解密方式为DES解密方式,和/或所述利用所述解密密钥解密所述加密屏体配置文件采用的解密方式为DES解密方式。

11.一种屏体配置文件导入装置,其特征在于,执行于播控设备,包括:

加密认证文件读取模块,用于响应导入指令以读取目标设备上的加密认证文件;

加密认证文件解密模块,用于利用解密密钥解密所述加密认证文件得到认证文件;

认证密码解密模块,用于读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码得到认证密码;以及

屏体配置文件解密模块,用于当所述认证密码与所述播控设备接收或存储的认证密码一致时,读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件,得到屏体配置文件以用于屏体配置;

其中,所述异或码和所述解密密钥为动态生成。

12.一种播控设备,用于对显示屏进行屏体配置;其特征在于,所述播控设备包括嵌入式处理器和存储器;其中所述存储器存储有供所述嵌入式处理器执行的指令,且所述指令使得所述嵌入式处理器执行操作以实现如权利要求9或10所述的屏体配置文件导入方法。

屏体配置文件导出、导入方法及其装置和播控设备

技术领域

[0001] 本发明涉及文件处理及媒体播放技术领域,尤其涉及一种屏体配置文件导出方法、一种屏体配置文件导出装置、一种屏体配置文件导入方法、一种屏体配置文件导入装置和一种播控设备。

背景技术

[0002] 播控设备例如多媒体播放盒具备屏体配置文件导出、导入功能,以用于更新显示屏例如LED显示屏的屏体配置信息。通常屏体管理员用U盘将屏体配置文件从其他设备(例如PC机等)导出,再将屏体配置文件导入到播控设备中以更新屏体配置。但这也给不法分子提供了采用同样的方式篡改显示屏的屏体配置的可能。解决该问题的传统的方法是将播控设备锁在密闭箱体内以避免不法分子接触到播控设备。然而该方法还是存在防护性能差、可靠性低的问题,依然有可能导致显示屏的屏体配置被篡改。

发明内容

[0003] 本发明实施例提供了一种屏体配置文件导出方法及其装置、一种屏体配置文件导入方法及其装置和一种播控设备,可以提高显示屏屏体配置的高防护性和高可靠性。

[0004] 一方面,本发明实施例提供的一种屏体配置文件导出方法,包括:响应导出指令以获取认证密码;利用异或码对所述认证密码进行加密运算得到加密认证密码;保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件;读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件;以及导出所述加密认证文件和所述加密屏体配置文件至目标设备。

[0005] 在本发明的一个实施例中,所述屏体配置文件包括屏体总带载大小、单个网口带载屏体数量、屏体走线方式和/或单个屏体大小。

[0006] 在本发明的一个实施例中,所述利用加密密钥加密所述认证文件得到加密认证文件采用的加密方式为DES加密方式,和/或所述利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件采用的加密方式为DES加密方式。

[0007] 在本发明的一个实施例中,所述异或码和所述加密密钥为动态生成;在所述导出所述加密认证文件和所述加密屏体配置文件至目标设备之后,所述屏体配置文件导出方法还包括:发送所述异或码和所述加密密钥以供播控设备获取;其中所述目标设备为用于向所述播控设备导入所述加密认证文件和所述加密屏体配置文件的移动存储设备,或者所述目标设备为所述播控设备。

[0008] 另一方面,本发明实施例提供的一种屏体配置文件导出装置,包括:认证密码获取模块,用于响应导出指令以获取认证密码;认证密码加密模块,用于利用异或码对所述认证密码进行加密运算得到加密认证密码;认证文件加密模块,用于保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件;屏体配置文件加密模块,用于读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文

件;以及文件导出模块,用于导出所述加密认证文件和所述加密屏体配置文件至目标设备。

[0009] 在本发明的一个实施例中,所述屏体配置文件包括屏体总带载大小、单个网口带载屏体数量、屏体走线方式和/或单个屏体大小。

[0010] 在本发明的一个实施例中,所述认证文件加密模块具体用于利用所述加密密钥并采用DES加密方式加密所述认证文件得到所述加密认证文件,和/或所述屏体配置文件加密模块具体用于利用所述加密密钥并采用DES加密方式加密所述屏体配置文件得到所述加密屏体配置文件。

[0011] 在本发明的一个实施例中,所述异或码和所述加密密钥为动态生成;所述屏体配置文件导出装置还包括:密码发送模块,用于发送所述异或码和所述加密密钥以供播控设备获取;其中所述目标设备为用于向所述播控设备导入所述加密认证文件和所述加密屏体配置文件的移动存储设备,或者所述目标设备为所述播控设备。

[0012] 又一方面,本发明实施例提供的一种屏体配置文件导入方法,包括:响应导入指令以读取目标设备上的加密认证文件;利用解密密钥解密所述加密认证文件得到认证文件;读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码得到认证密码;以及当所述认证密码与认证密码一致时,读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件,得到屏体配置文件以用于屏体配置。

[0013] 在本发明的一个实施例中,所述利用解密密钥解密所述加密认证文件得到认证文件采用的解密方式为DES解密方式,和/或所述利用所述解密密钥解密所述加密屏体配置文件采用的解密方式为DES解密方式。

[0014] 又一方面,本发明实施例提供的一种屏体配置文件导入装置,包括:加密认证文件读取模块,用于响应导入指令以读取目标设备上的加密认证文件;加密认证文件解密模块,用于利用解密密钥解密所述加密认证文件得到认证文件;认证密码解密模块,用于读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码得到认证密码;以及屏体配置文件解密模块,用于当所述认证密码与认证密码一致时,读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件,得到屏体配置文件以用于屏体配置。

[0015] 再一方面,本发明实施例提供的一种播控设备,用于对显示屏进行屏体配置;所述播控设备包括嵌入式处理器和存储器;其中所述存储器存储有供所述嵌入式处理器执行的指令,且所述指令使得所述嵌入式处理器执行操作以实现如前述的屏体配置文件导入方法。

[0016] 上述一个或多个技术方案可以具有如下优点或有益效果:本发明实施例通过对认证密码进行两次加密、解密,和对屏体配置文件进行一次加密、解密,确保只能由指定人员(显示屏管理人员)完成屏体配置文件导出、导入操作,避免了不法分子篡改显示屏的屏体配置信息的可能,提升了播控设备的屏体配置文件更新过程的高防护性和高可靠性。

附图说明

[0017] 为了更清楚地说明本发明实施例的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本发明的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的

附图。

[0018] 图1为本发明第一实施例提供的一种屏体配置文件导出方法的流程示意图。

[0019] 图2为本发明第二实施例提供的一种屏体配置文件导出装置的结构示意图。

[0020] 图3为本发明第三实施例提供的一种屏体配置文件导入方法的流程示意图。

[0021] 图4为本发明第四实施例提供的一种屏体配置文件导入装置的结构示意图。

[0022] 图5为本发明第五实施例提供的一种播控设备的结构示意图。

具体实施方式

[0023] 下面将结合本发明实施例中的附图,对本发明实施例中的技术方案进行清楚、完整地描述,显然,所描述的实施例仅仅是本发明一部分实施例,而不是全部的实施例。基于本发明中的实施例,本领域普通技术人员在没有作出创造性劳动前提下所获得的所有其他实施例,都属于本发明保护的范围。

[0024] 【第一实施例】

[0025] 如图1所示,本发明第一实施例提供的一种屏体配置文件导出方法,例如包括步骤:

[0026] S11:响应导出指令以获取认证密码;

[0027] S13:利用异或码对所述认证密码进行加密运算得到加密认证密码;以及

[0028] S15:保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件;

[0029] S17:读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件;以及

[0030] S19:导出所述加密认证文件和所述加密屏体配置文件至目标设备。

[0031] 为便于理解本发明,下面将对本实施例的屏体配置文件导出方法的各个步骤进行详细描述。

[0032] 播控设备例如多媒体播放盒具备屏体配置文件导出、导入功能以更新显示屏的屏体配置。此处的屏体配置文件例如包括屏体总带载大小如多个屏体拼接后形成的大屏的总带载大小、单个网口屏体带载数量、屏体走线方式(或称屏体间的连线方式)和/或单个屏体大小如分辨率等。但在向播控设备导入屏体配置文件之前,需要从上位机导出所述屏体配置文件。本实施例的屏体配置文件导出方法通常用上位机上的屏体配置文件导出软件例实现的,例如通过使用多重加密密码来对需要导出的屏体配置文件进行加密和保护。然后,在屏体配置文件导入到播控设备的时候,需要对屏体配置文件进行合法性验证例如利用对应的多重解密密码校验通过后才能将屏体配置文件导入。多重加密密码的密码和多重解密密码中对应的密码可以相同,也可以不相同,仅需能配对使用即可。例如,多重加密密码例如包括认证密码、异或码和加密密钥。多重加密密码中的异或码和加密密钥用于对认证密码进行两次加密。多重解密密码例如包括认证密码、异或码和解密密钥。多重解密密码中的异或码和解密密钥用于对加密后的文件进行解密以得到认证密码。此处的多重加密密码中的认证密码和多重解密密码的认证密码相同,用于在导入屏体配置文件时的身份校验。多重加密密码中的异或码和多重解密密码的异或码相同。多重加密密码中的加密密钥和多重解密密码的解密密钥是否相同,可根据不同的加密解密方式而定,例如采用DES(Data

Encryption Standard,数据加密标准)方式时,加密密钥和解密密钥相同。

[0033] 多重加密密码中的异或码和加密密钥以及对应的多重解密密码中的异或码和解密密钥可以提前配置或约定,也可以动态配置。提前配置指的是提前生成多重加密密码中的异或码和加密密钥以及对应的多重解密密码中的异或码和解密密钥,并提前存储至PC机和相应的播控设备中以供获取和使用,后期每次导出、导入操作都使用相同的多重加密密码和多重解密密码。

[0034] 动态配置指的是上位机和目标播控设备通过互联网、局域网、WIFI、蓝牙或lora等连接,上位机即时生成多重加密密码中的异或码和加密密钥以及对应的多重解密密码中的异或码和解密密钥、并通过网络将多重解密密码中的异或码和解密密钥发送至指定的多媒体播放盒如异步播放盒。此处值得一提的是,多重加密密码中的认证密码和多重解密密码的认证密码均在PC机和播控设备上预先设定或约定好。上位机利用异或码和加密密钥加密多重加密密码中的认证密码以及屏体配置文件,然后将加密后的认证密码文件和屏体配置文件导出至目标设备例如移动存储设备如U盘、并将多重解密密码中的异或码和解密密钥发送给目标播控设备,再将U盘中加密后的认证密码文件和屏体配置文件进行解密后导入到目标播控设备。又例如,上位机利用多重加密密码中的异或码和加密密钥加密认证密码和屏体配置文件,然后将加密后的认证密码文件和屏体配置文件导出至目标设备例如U盘、之后将多重解密密码中的异或码和解密密钥发送至服务器;当屏体管理人员将存有加密后的认证密码文件和屏体配置文件的U盘连接到目标播控设备时,目标播控设备从服务器获取多重解密密码中的异或码和解密密钥并对需要导入的屏体配置文件进行解密后导入到目标播控设备。此处值得一提的是,多重加密密码和对应的多重加密密码中的异或码和加密密钥、多重解密密码中异或码和解密密钥为随机生成,可提高密码本身的保密性和屏体配置文件的高防护性和高可靠性。另外,由于每次生成的多重加密密码和对应的多重解密密码可以与其它次生成的密码不相同,也即每次导出和导入操作使用的多重加密密码中的异或码和加密密钥以及多重解密密码的异或码解密密钥各不相同,这样进一步提高屏体配置文件的高防护性和高可靠性。

[0035] 下面以多重加密密码中的认证密码与多重解密密码中的认证密码相同、多重加密密码中的异或码和多重解密密码中的异或码相同、多重加密密码中的加密密钥与多重解密密钥中的解密密钥相同为例说明本发明实施例提供的屏体配置文件的导出方法。

[0036] 首先,响应屏体配置文件导出指令以获取认证密码。当需要导出屏体配置文件时,屏体管理员在屏体配置文件导出软件上进行屏体配置文件导出操作,屏体配置文件导出软件响应屏体配置文件导出指令以获取认证密码。具体地,屏体配置文件导出软件响应屏体配置文件导出指令,自动显示输入界面以供用户输入事先约定的认证密码。在用户输入认证密码并确认后,响应用户操作指令读取认证密码。此处的认证密码用于在向播控设备导入屏体配置文件时校验屏体管理员身份合法性。

[0037] 然后,利用异或码对所述认证密码进行加密运算得到加密认证密码。具体包括:对认证密码与异或码进行异或运算,以完成认证密码的一次加密。当然也可以用异或码对认证密码进行其它的加密运算得到加密认证密码。

[0038] 之后,保存所述加密认证密码至文件得到认证文件,并利用加密密钥加密认证文件得到加密认证文件。这样就完成认证密码的二次加密。此处采用的加密方式可例如为对

称加密方式如DES加密方式,当然也可以采用其它的加密方式。

[0039] 其次,读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件。此处采用的加密方式也可例如为对称加密方式如DES加密方式,当然也可以采用其它的加密方式。

[0040] 最后,导出加密认证文件和加密屏体配置文件至目标设备。此处的目标设备可例如为移动存储设备如U盘、移动硬盘等。当然,目标设备也可以是屏体配置需要更新的播控设备,例如PC机通过网线连接播控设备,使得PC机可直接通过网络向播控设备发送加密认证文件和加密屏体配置文件、以及异或码和解密密钥。

[0041] 进一步地,在导出加密认证文件和加密屏体配置文件至目标设备之后,发送异或码和加密密钥以供目标播控设备获取。此处可以理解的是,PC机可直接将异或码和加密密钥发送至目标播控设备,也可以将异或码和加密密钥发送至服务器,以供与所述服务器相连的目标播控设备随时获取。此处的目标播控设备例如为需要更新屏体配置的播控设备。

[0042] 综上所述,本发明实施例通过对认证密码进行两次加密和对屏体配置文件进行一次加密,可确保屏体配置文件导出过程中的高防护性和高可靠性。另外,动态、随机生成多重加密密码中的异或码和加密密钥以及多重解密密码中的异或码和解密密钥,并在导出加密后的屏体配置文件后通过网络将异或码和解密密钥发送至目标播控设备上,可进一步提高屏体配置文件的高防护性和高可靠性。此外,每次导入、导出操作中动态生成不相同的密码,更进一步有利于屏体配置文件的保密和防护。

[0043] 【第二实施例】

[0044] 如图2所示,本发明第二实施例提供了一种屏体配置文件导出装置100。屏体配置文件导出装置100例如包括:认证密码获取模块110、认证密码加密模块130、认证文件加密模块150、屏体配置文件加密模块170和文件导出模块190。

[0045] 认证密码获取模块110,用于响应导出指令以获取认证密码。

[0046] 认证密码加密模块130,用于利用异或码对所述认证密码进行加密运算得到加密认证密码。

[0047] 认证文件加密模块150,用于保存所述加密认证密码至认证文件,并利用加密密钥加密所述认证文件得到加密认证文件。

[0048] 屏体配置文件加密模块170,用于读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件。以及

[0049] 文件导出模块190,用于导出所述加密认证文件和所述加密屏体配置文件至目标设备。

[0050] 进一步地,屏体配置文件导出装置100还包括密码发送模块120。密码发送模块120用于发送所述异或码和所述加密密钥以供播控设备获取;其中所述目标设备为用于向所述播控设备导入所述加密认证文件和所述加密屏体配置文件的移动存储设备,或者所述目标设备为所述播控设备。

[0051] 本实施例中的屏体配置文件导出装置100中的各模块之间的具体工作过程和技术效果参见前述第一实施例的描述。

[0052] 【第三实施例】

[0053] 如图3所示,本发明第三实施例提供的一种屏体配置文件导入方法例如包括步骤:

[0054] S31:响应导入指令以读取目标设备上的加密认证文件;

[0055] S33:利用解密密钥解密所述加密认证文件得到认证文件;

[0056] S35:读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码得到认证密码;以及

[0057] S37:当所述认证密码与认证密码一致时,读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件,得到屏体配置文件以用于屏体配置。

[0058] 为便于理解本发明,下面将对本实施例的屏体配置文件导入方法的各个步骤进行详细描述。

[0059] 承上述,当与播控设备连接的LED显示屏的屏体需要更新配置时,屏体管理员将新的屏体配置文件从目标设备导入到播控设备以通过播控设备来更新屏体配置。此处的目标设备可例如为移动存储设备如U盘、移动硬盘等。另外,目标设备也可以是存储有新的屏体配置文件的PC机。例如播控设备通过网络连接PC机,使得播控设备可直接通过网络从PC机导入屏体配置文件以更新屏体配置。为了确保导入屏体配置文件的合法性,需要对导入的屏体配置文件进行合法性验证,确保其高防护性和高可靠性。本实施例的屏体配置文件导入方法可通过播控设备上的终端软件实现,例如通过使用的密码来验证需要导入文件的合法性。下面以U盘为例说明本实施例提供的屏体配置文件导入方法。

[0060] 响应屏体配置文件导入指令读取目标设备上的加密认证文件。当需要导入屏体配置文件时,屏体管理员将U盘连接目标播控设备。屏体管理员在播控设备上进行相应的操作例如单击屏体配置文件导入按钮后,播控设备上的终端程序响应用户操作指令读取U盘内的加密认证文件。此处的加密认证文件可例如为本发明第一实施例中的加密认证文件。当然,在读取目标设备上的加密认证文件之前,需要先预设或者约定认证密码,以及获取异或码和解密密钥。例如从PC机或服务器上通过如互联网、局域网、WIFI、蓝牙或lora等方式接收异或码和解密密钥。此处的异或码和解密密钥分别与本发明第一实施例中的异或码和加密密钥一一对应,甚至相同。

[0061] 利用解密密钥解密所述加密认证文件得到认证文件。此处采用的解密方式可例如为DES解密方式,当然也可以采用其它的解密方式。这样一来就完成了认证密码的一次解密。

[0062] 读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码,具体包括:将所述加密认证密码与预先设定的异或码进行异或运算。这样就完成了认证密码的二次解密。

[0063] 判断解密后的认证密码是否与播控设备接收或存储的认证密码是否一致。当所述认证密码与认证密码不一致时,表明身份校验失败,意味着此次屏体配置文件导入操作不是屏体管理员执行的,终端程序则立即终止屏体配置文件导入流程。当所述认证密码与认证密码一致时,表明身份验证成功,意味着此次屏体配置文件导入操作是屏体管理员执行的,然后读取U盘内的加密屏体配置文件,并利用解密密钥解密所述加密屏体配置文件。此处采用的解密方式可例如为DES解密方式,当然也可以采用其它的解密方式。当成功解密所述加密屏体配置文件得到屏体配置文件时,则导入屏体配置文件,然后播控设备则按照屏体配置文件对LED显示屏进行配置。当解密所述加密屏体配置文件没有到屏体配置文件时,表明屏体配置文件不合法,终端程序立即终止屏体配置文件导入流程。

[0064] 综上所述,本发明实施例通对认证密码进行两次解密和对屏体配置文件进行一次解密,可确保只能由指定人员(显示屏管理人员)通过目标设备完成屏体配置文件导入操作,避免了不法分子篡改显示屏播放节目的可能,提升了播控设备的屏体配置文件更新过程的高防护性和高可靠性。

[0065] 【第四实施例】

[0066] 如图4所示,本发明第四实施例提供一种屏体配置文件导入装置300。屏体配置文件导入装置300例如包括:加密认证文件读取模块310、加密认证文件解密模块330、认证密码解密模块350以及屏体配置文件解密模块370。

[0067] 加密认证文件读取模块310,用于响应导入指令以读取目标设备上的加密认证文件;

[0068] 加密认证文件解密模块330,用于利用解密密钥解密所述加密认证文件得到认证文件;

[0069] 认证密码解密模块350,用于读取所述认证文件中的加密认证密码,并利用异或码解密所述加密认证密码得到认证密码;以及

[0070] 屏体配置文件解密模块370,用于当所述认证密码与认证密码一致时,读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件,得到屏体配置文件以用于屏体配置。

[0071] 进一步地,屏体配置文件导入装置300还包括密码获取模块(图中未示出)。密码获取模块用于获取所述异或码和所述加密密钥。

[0072] 本实施例中的屏体配置文件导入装置300的具体工作过程和技术效果参见前述第三实施例的描述。

[0073] 【第五实施例】

[0074] 如图5所示,本发明第五实施例提供一种用于对LED显示屏进行屏体配置的播控设备500如异步多媒体播放盒。播控设备500例如包括嵌入式处理器510和存储器530。其中,存储器530存储有供嵌入式处理器510执行的指令531。嵌入式处理器510执行指令531以实现如前述第三实施例提供的屏体配置文件导入方法。

[0075] 本实施例中的播控设备500的具体工作过程和技术效果参见前述第三实施例的描述,此处不再赘述。

[0076] 在本发明所提供的几个实施例中,应该理解到,所揭露的系统,装置和方法,可以通过其它的方式实现。例如,以上所描述的装置实施例仅仅是示意性的,例如,单元的划分,仅仅为一种逻辑功能划分,实际实现时可以有另外的划分方式,例如多路单元或组件可以结合或者可以集成到另一个系统,或一些特征可以忽略,或不执行。另一点,所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口,装置或单元的间接耦合或通信连接,可以是电性,机械或其它的形式。

[0077] 作为分离部件说明的单元可以是或者也可以不是物理上分开的,作为单元显示的部件可以是或者也可以不是物理单元,即可以位于一个地方,或者也可以分布到多路网络单元上。可以根据实际的需要选择其中的部分或者全部单元来实现本实施例方案的目的。

[0078] 最后应说明的是:以上实施例仅用以说明本发明的技术方案,而非对其限制;尽管参照前述实施例对本发明进行了详细的说明,本领域的普通技术人员应当理解:其依然可

以对前述各实施例所记载的技术方案进行修改,或者对其中部分技术特征进行等同替换;而这些修改或者替换,并不使相应技术方案的本质脱离本发明各实施例技术方案的精神和范围。

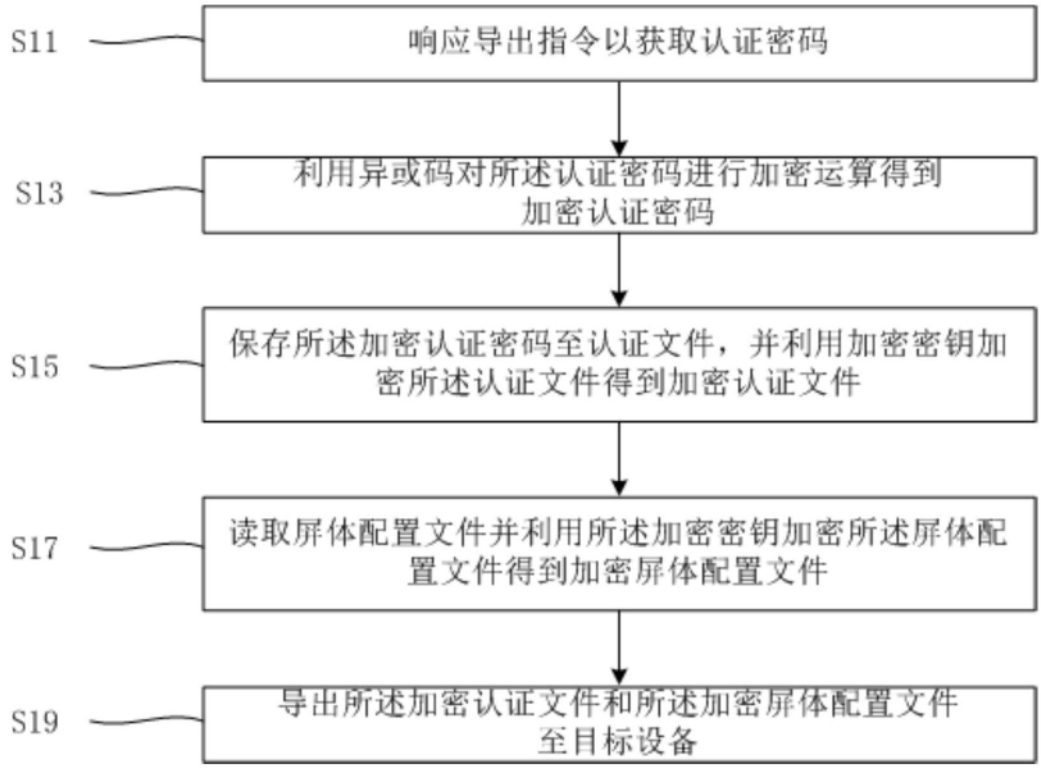

S11
响应导出指令以获取认证密码
S13
利用异或码对所述认证密码进行加密运算得到加密认证密码
S15
保存所述加密认证密码至认证文件，并利用加密密钥加密所述认证文件得到加密认证文件
S17
读取屏体配置文件并利用所述加密密钥加密所述屏体配置文件得到加密屏体配置文件
S19
导出所述加密认证文件和所述加密屏体配置文件至目标设备

图1

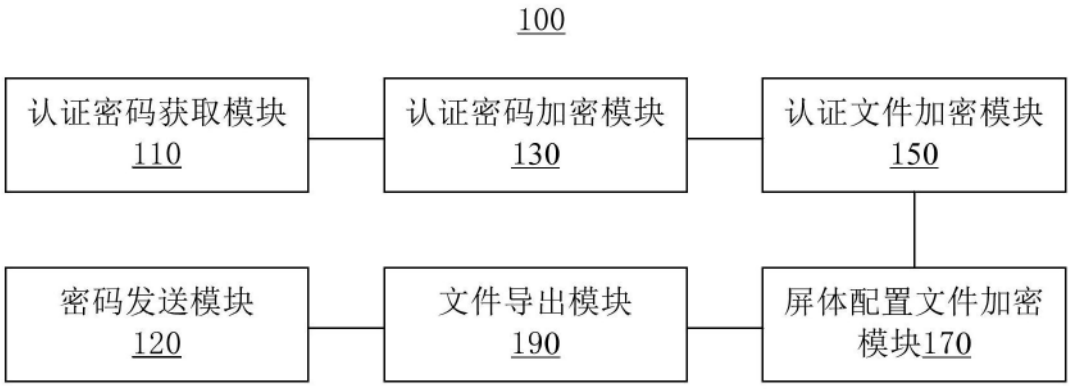

100
认证密码获取模块 110
认证密码加密模块 130
认证文件加密模块 150
密码发送模块 120
文件导出模块 190
屏体配置文件加密模块170

图2

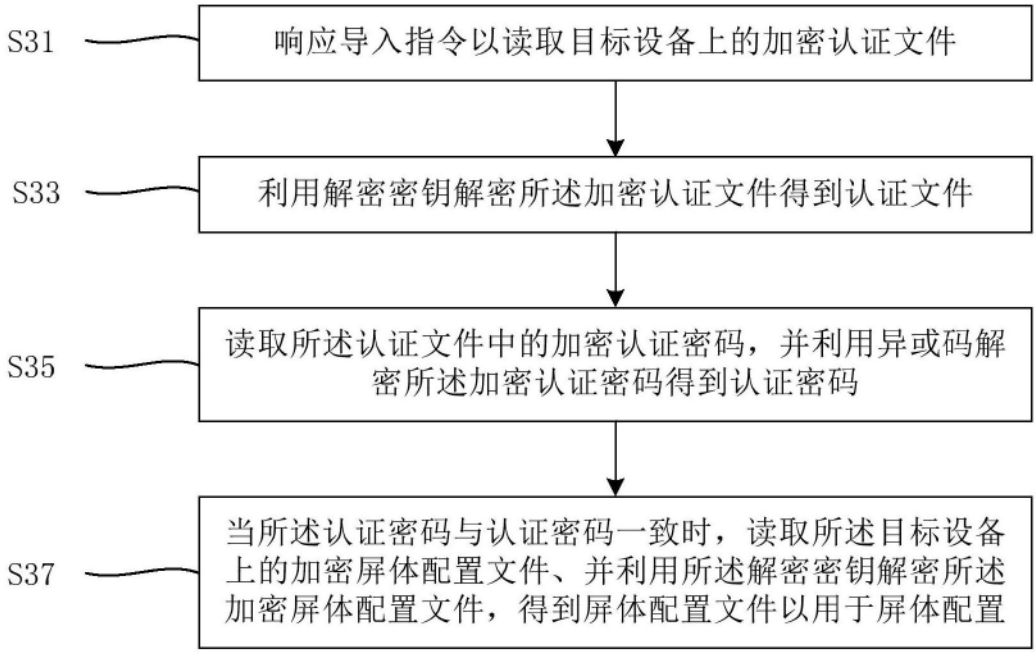

S31
响应导入指令以读取目标设备上的加密认证文件
S33
利用解密密钥解密所述加密认证文件得到认证文件
S35
读取所述认证文件中的加密认证密码，并利用异或码解密所述加密认证密码得到认证密码
S37
当所述认证密码与认证密码一致时，读取所述目标设备上的加密屏体配置文件、并利用所述解密密钥解密所述加密屏体配置文件，得到屏体配置文件以用于屏体配置

图3

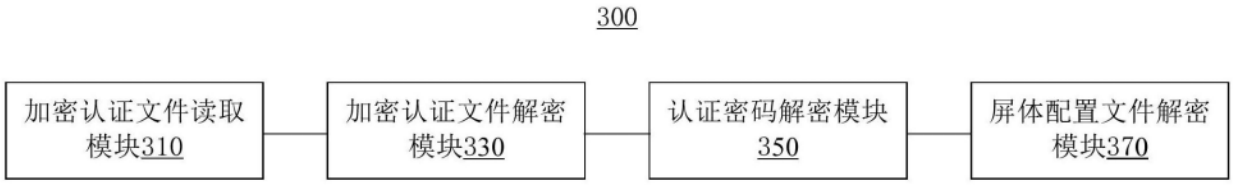

300
加密认证文件读取模块310
加密认证文件解密模块330
认证密码解密模块350
屏体配置文件解密模块370

图4

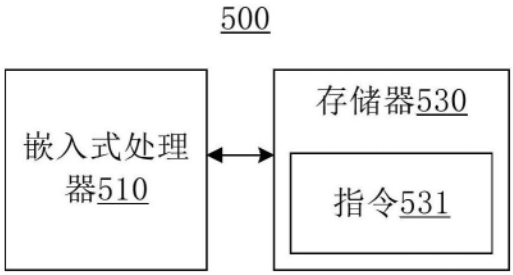

500
嵌入式处理器510
存储器530
指令531

图5