



(12) 发明专利申请

(10) 申请公布号 CN 103413518 A

(43) 申请公布日 2013. 11. 27

(21) 申请号 201310277326. 4

G06F 3/14(2006. 01)

(22) 申请日 2013. 07. 03

(71) 申请人 深圳市奥拓电子股份有限公司

地址 518000 广东省深圳市南山区高新技术产业园南园 T2 栋 A6-B

(72) 发明人 沈毅 王利强 梁德斌 吴振志
刘玲 吴涵渠

(74) 专利代理机构 深圳市凯达知识产权事务所
44256

代理人 刘大弯

(51) Int. Cl.

G09G 3/32(2006. 01)

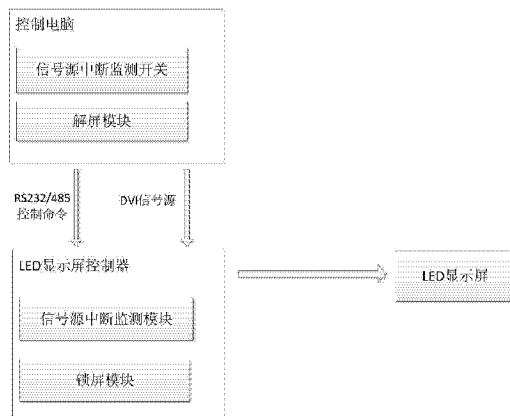
权利要求书1页 说明书3页 附图2页

(54) 发明名称

一种 LED 显示屏系统及其控制信号源安全的方法

(57) 摘要

本发明公开了一种 LED 显示屏系统及其控制信号源安全的方法。该系统包括顺序连接的控制电脑、LED 显示屏控制器和 LED 显示屏 ;LED 显示屏控制器具有 :用于实时监测输入的信号源是否发生了中断的信号源中断监测模块 ;用于在信号源中断监测模块监测到输入的信号源发生中断时进行锁屏的锁屏模块 ;且控制电脑具有可解除锁屏状态的解屏模块。采用了本发明技术方案控制信号源安全方法的一种 LED 显示屏系统,不法分子切换信号源的时候,信号源中断监测模块必然可以检测到信号源发生了中断,从而触发锁屏模块动作,将 LED 显示屏所显示的画面定格在信号源中断前所显示画面的最后一帧,确保非法信号源的图像不会在 LED 显示屏上显示,从而确保 LED 显示屏所发布信息 and 画面的安全。



1. 一种 LED 显示屏系统,包括顺序连接的:控制电脑、LED 显示屏控制器和 LED 显示屏,其特征在于,所述 LED 显示屏控制器具有:用于实时监测输入的信号源是否发生了中断的信号源中断监测模块;用于在信号源中断监测模块监测到输入的信号源发生中断时进行锁屏的锁屏模块;且所述控制电脑具有可解除锁屏状态的解屏模块,用于在非法入侵的可能性被排除后解除锁屏模块的锁屏以恢复正常播放。

2. 如权利要求 1 所述的一种 LED 显示屏系统,其特征在于,所述控制电脑还具有可用于控制所述信号源中断监测模块开/关的信号源中断监测开关。

3. 如权利要求 1 或 2 所述的一种 LED 显示屏系统,其特征在于,所述锁屏是指将 LED 显示屏所显示画面定格在中断前的最后一帧。

4. 一种 LED 显示屏系统控制信号源安全的方法,其基于权利要求 1 所述的一种 LED 显示屏系统来控制信号源的安全,该方法包括如下步骤:

S1)、监测:系统上电运行后,信号源中断监测模块实时监测输入进 LED 显示屏控制器的信号源是否发生了中断;

S2)、锁屏:信号源中断监测模块一旦监测到信号源发生中断,则触发锁屏模块将 LED 显示屏所显示的画面定格在中断前的最后一帧;

S3)、解屏:非法入侵的可能性被排除后,所述解屏模块解除锁屏模块的锁屏,从而恢复 LED 显示屏系统的正常播放。

5. 如权利要求 4 所述的一种 LED 显示屏系统控制信号源安全的方法,其特征在于,所述控制电脑还具有可用于控制所述信号源中断监测模块开/关的信号源中断监测开关;该方法包括“暂时屏蔽保护”的步骤:在信号源合法中断之前,通过该信号源中断监测开关暂时关闭信号源中断监测模块,所述信号源合法中断包括但不限于的合法切换信号源以及合法维护 LED 显示屏系统。

6. 如权利要求 4 或 5 所述的一种 LED 显示屏系统控制信号源安全的方法,其特征在于,所述锁屏是指将 LED 显示屏所显示画面定格在中断前的最后一帧。

一种 LED 显示屏系统及其控制信号源安全的方法

技术领域

[0001] 本发明涉及 LED 显示技术领域,具体涉及一种 LED 显示屏系统及其控制信号源安全的方法。

背景技术

[0002] 近年来 LED 显示技术发展迅速,各种各样的 LED 大屏已经越来越多的进入人们的视野。目前的 LED 显示屏系统一般如图 1 所示,控制电脑通过 RS232/485 串口以及 DVI 接口与 LED 显示屏控制器连接,而 LED 显示屏控制器再与 LED 显示屏连接。控制电脑上安装有 LED 显示屏控制软件,负责提供节目信号源。LED 显示屏控制器又称 LED 显示屏控制卡,它是组成 LED 显示屏系统的核心部件,主要负责接收来自控制电脑串口的控制命令和 DVI 接口的信号源。而 LED 显示屏接受 LED 显示屏控制器的控制,并显示信号源提供的画面。

[0003] 在上述的 LED 显示屏系统中,控制电脑通过 RS232/485 串口发送控制命令,控制 LED 显示屏的开 / 关屏、亮度调节、色温等屏体参数。同时通过 DVI 接口将信号源发送给 LED 显示屏控制器。存在的问题是,在 LED 显示屏系统正在运行时,允许用户改变信号源。比如:断开控制电脑显卡通过 DVI 接口发送的信号源,改用 DVD 播放器输出的信号源。信号源切换之后,LED 显示屏控制器可以继续接收新的信号源,并控制 LED 显示屏显示新信号源的节目画面。上述技术方案中,因为对信号源的切换没有加以限制,由此可能带来严重的安全问题,比如入侵设备可以通过攻击 LED 显示屏信号源进行非法内容宣传。不法分子不用攻破控制电脑的使用权限,仅仅需要将 DVI 线缆从控制电脑拔下,连接到自己入侵设备即可到达目的。如图 2 所示,法轮功或者恐怖主义的不法分子切断 LED 显示屏系统合法的信号源,再使用一台入侵设备(PC 机或者 DVD 播放机)将非法的信号源输出给 LED 显示屏控制器,就会造成入侵设备提供的非法内容在 LED 显示屏上播放,从而有可能扰乱社会次序,并可能造成骚乱等严重后果。

[0004] 综上所述,现有 LED 显示屏系统无法控制信号源的安全,容易给不法分子可乘之机,存在重大安全隐患,因而需要改进。

发明内容

[0005] 本发明所要解决的技术问题之一是提供一种 LED 显示屏系统,其能够控制信号源的安全,克服现有 LED 显示屏系统容易给不法分子入侵 LED 显示屏系统可乘之机的安全隐患。

[0006] 为解决上述技术问题,本发明采用如下技术方案:

[0007] 一种 LED 显示屏系统,包括顺序连接的控制电脑、LED 显示屏控制器和 LED 显示屏;所述 LED 显示屏控制器具有:用于实时监测输入的信号源是否发生了中断的信号源中断监测模块;用于在信号源中断监测模块监测到输入的信号源发生中断时进行锁屏的锁屏模块;且所述控制电脑具有可解除锁屏状态的解屏模块,用于在非法入侵的可能性被排除后解除锁屏模块的锁屏以恢复正常播放。

[0008] 优选的技术方案中,所述控制电脑还具有可用于控制所述信号源中断监测模块开/关的信号源中断监测开关。

[0009] 优选的技术方案中,所述锁屏是指将 LED 显示屏所显示画面定格在中断前的最后一帧。

[0010] 本发明所要解决的技术问题之二是相应提供一种 LED 显示屏系统控制信号源安全的方法,其能够控制信号源的安全,克服现有 LED 显示屏系统容易给不法分子入侵 LED 显示屏系统可乘之机的安全隐患。

[0011] 为解决上述技术问题,本发明采用如下技术方案:

[0012] 一种 LED 显示屏系统控制信号源安全的方法,其基于前述的一种 LED 显示屏系统来控制信号源的安全,该方法包括如下步骤:

[0013] S1)、监测:系统上电运行后,信号源中断监测模块实时监测输入进 LED 显示屏控制器的信号源是否发生了中断;

[0014] S2)、锁屏:信号源中断监测模块一旦监测到信号源发生中断,则触发锁屏模块将 LED 显示屏所显示的画面定格在中断前的最后一帧;

[0015] S3)、解屏:非法入侵的可能性被排除后,所述解屏模块解除锁屏模块的锁屏,从而恢复 LED 显示屏系统的正常播放。

[0016] 优选的技术方案中,所述控制电脑还具有可用于控制所述信号源中断监测模块开/关的信号源中断监测开关;该方法包括“暂时屏蔽保护”的步骤:在信号源合法中断之前,通过该信号源中断监测开关暂时关闭信号源中断监测模块,所述信号源合法中断包括但不限于的合法切换信号源以及合法维护 LED 显示屏系统。

[0017] 优选的技术方案中,所述锁屏是指将 LED 显示屏所显示画面定格在中断前的最后一帧。

[0018] 本发明的有益效果是:采用了本发明技术方案一种 LED 显示屏系统控制信号源安全的方法的一种 LED 显示屏系统,不法分子切换信号源的时候,信号源中断监测模块必然可以检测到信号源发生了中断,从而触发锁屏模块动作,将 LED 显示屏所显示的画面定格在信号源中断前所显示画面的最后一帧,确保非法信号源的图像不会在 LED 显示屏上显示,从而确保 LED 显示屏所发布信息 and 画面的安全。入侵排除后,可以使用解屏模块,解除 LED 显示屏的锁定状态,恢复正常播放。

附图说明

[0019] 图 1 是现有 LED 显示屏系统的原理框图;

[0020] 图 2 是不法分子入侵现有 LED 显示屏系统的示意图;

[0021] 图 3 是本发明具体实施方式 LED 显示屏系统的原理框图。

[0022] 下面将结合附图对本发明作进一步详述。

具体实施方式

[0023] 为了避免不法分子利用入侵设备非法切换 LED 显示屏系统的信号源,从而避免 LED 显示屏系统播放非法的信息,本具体实施方式提供的一种 LED 显示屏系统如图 3 所示,和现有 LED 显示屏系统一样,也包括:控制电脑、LED 显示屏控制器和 LED 显示屏。和现有

技术的不同之处在于,控制电脑中还包括:解屏模块;而LED显示屏控制器中则增设了信号源中断监测模块和锁屏模块。

[0024] 其中:信号源中断监测模块用于实时监测输入进来的信号源是否发生了中断;锁屏模块,用于在信号源中断监测模块监测到输入进来的信号源发生中断时,将LED显示屏所显示的画面定格在中断前最后一帧,锁定在最后一帧可以使得LED显示屏不至于黑屏或者显示其它不合适的画面;解屏模块用于解除锁屏模块的锁屏动作。这样,当不法分子切换信号源的时候,信号源中断监测模块必然可以检测到信号源发生了中断,从而触发锁屏模块动作,将LED显示屏所显示的画面定格在信号源中断前所显示画面的最后一帧,确保非法信号源的图像不会在LED显示屏上显示,从而确保LED显示屏所发布信息 and 画面的安全。入侵排除后,可以使用解屏模块,解除LED显示屏的锁定状态,恢复正常播放。

[0025] LED显示屏作为一种受众广、影响大的宣传媒介,其播放内容的安全性不容忽视。本发明具体实施方式可以防范入侵设备通过攻击LED显示屏信号源进行非法内容宣传,增强LED显示屏的健康、积极宣传效果,具有较大的实用价值。

[0026] 但是,前述的技术方案中容易发生误动作,比如在合法切换信号源或者对LED显示屏进行合法维护时,也可能触发锁屏模块动作,这时可能需要频繁通过解屏模块进行解屏使系统再次正常工作,因而可能存在不便。优选的技术方案中,还在控制电脑上增设了信号源中断监测开关,该信号源中断监测开关用于控制所述信号源中断监测模块的开关。在进行合法切换以及正常维护需要时,可以通过该信号源中断检测开关来关闭所述信号源中断监测模块,LED显示屏系统正常工作时,则通过该信号源中断检测开关来开启所述信号源中断监测模块。

[0027] 需要强调说明的是,本领域中一般技术人员都可以理解以上所述:信号源中断监测开关、解屏模块、信号源中断监测模块和锁屏模块可以通过硬件去实现,也可以在一定硬件基础上通过软件去实现,也可以通过软硬件结合去实现。不过在目前技术条件下,信号源中断监测开关和解屏模块在控制电脑的控制软件上去实现更为简单和方便。而信号源中断监测模块和锁屏模块可以通过软件实现,亦可以通过硬件实现,优选通过软硬件结合的方式实现,本文在此不再详述,但是这些实现方式都应该在本发明的保护范围之内。

[0028] 以上内容是结合具体的优选实施方式对本发明所作的进一步详细说明,不能认定本发明的具体实施只局限于这些说明。对于本发明所属技术领域的普通技术人员来说,在不脱离本发明构思的前提下,还可以做出若干简单推演或替换,都应当视为属于本发明的保护范围。

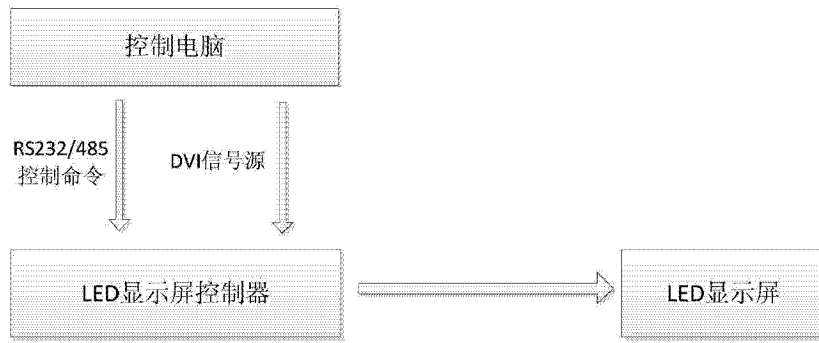


图 1

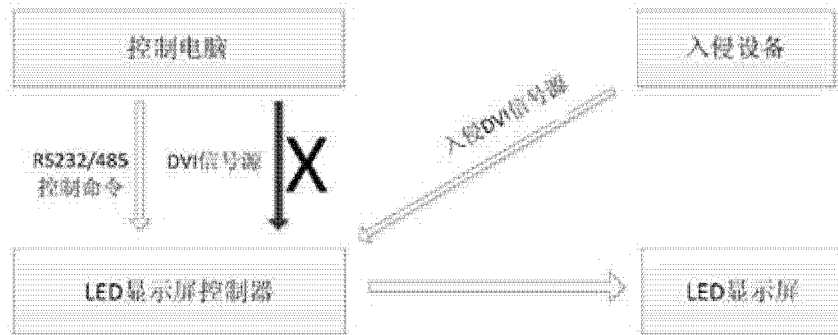


图 2

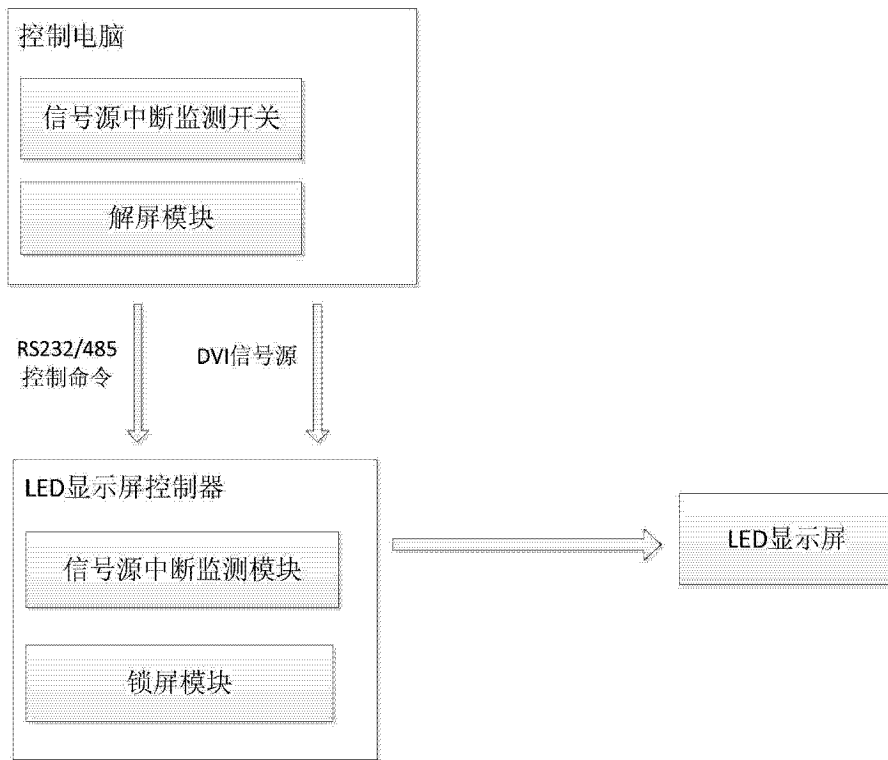


图 3