发明名称
实时锁屏系统

摘要
本发明涉及一种实时锁屏系统，该系统的自动运行模块用于使锁屏系统随操作系统自动运行，密码初始化模块用于读取配置文件中加密的用户密码，解密后对用户密码进行初始化；加锁模块包括锁屏模块和安装鼠标键盘钩子模块；消息阻断模块利用鼠标键盘钩子阻断鼠标和键盘消息，并且判断用户输入的按键是否与鼠标键盘钩子中的解锁按键相同，若相同则解锁键盘，允许输入用户密码，否则阻断鼠标和键盘消息；密码认证模块用于判别用户输入的密码是否与用户密码相符，是则由解锁模块解除锁屏操作，卸载鼠标键盘钩子。本发明可适用于保护的 Windows 操作系统，安全度高、运行稳定性好，开发和维护成本低。
1. 一种实时锁屏系统，其特征在于包括自动运行模块，密码初始化模块，加锁模块，消息阻断模块，密码认证模块，解锁模块；所述自动运行模块用于使锁屏系统随操作系统自动运行；密码初始化模块用于读取配置文件中加密的用户密码，解密后对用户密码进行初始化；加锁模块包括锁屏模块和安装鼠标键盘键子模块；消息阻断模块利用鼠标键盘键子阻断鼠标和键盘消息，并且判断用户输入的按键是否与鼠标键盘键子中的解锁按键相同，若相同则解锁键盘，允许输入用户密码，否则阻断鼠标和键盘消息；密码认证模块用于判断用户输入的密码是否与用户密码相符，是则由解锁模块解除锁屏操作，卸载鼠标键盘键子。

2. 根据权利要求1所述的实时锁屏系统，其特征在于所述密码初始化模块还用于初始化超级密码。

3. 根据权利要求1所述的实时锁屏系统，其特征在于还包括托盘伺服模块和密码设置模块；所述托盘伺服模块用于锁屏状态下等待用户的加锁、解密设置和退出操作；密码设置模块用于设置用户密码，并将用户密码加密后保存到配置文件。

4. 根据权利要求1、2或3所述的实时锁屏系统，其特征在于所述锁屏模块包括一用于最大化程序主窗口，使其置顶，并且透明的子模块；解锁模块包括一用于最小化程序主窗口的子模块。

5. 根据权利要求1、2或3所述的实时锁屏系统，其特征在于所述锁屏模块包括一用于隐藏，锁定任务栏的子模块；解锁模块包括一用于任务栏解锁的子模块。

6. 根据权利要求1、2或3所述的实时锁屏系统，其特征在于所述锁屏模块包括一用于任务管理器锁定的子模块；解锁模块包括一用于任务管理器解锁的子模块。

7. 根据权利要求1、2或3所述的实时锁屏系统，其特征在于所述任务管理器锁定子模块，用于修改注册表，禁止任务管理器；或利用第一定时器随时关闭任务管理器窗口；或修改注册表，禁止任务管理器的同时打开第一定时器，随时关闭任务管理器窗口；任务管理器解锁子模块，用于修改注册表，打开任务管理器；或关闭第一定时器，解除任务管理器的锁定；或修改注册表，打开任务管理器，同时关闭第一定时器，解除任务管理器的锁定。

8. 根据权利要求1、2或3所述的实时锁屏系统，其特征在于所述锁屏模块包括一用于开启第一定时器，将鼠标位置设定到屏幕范围之外，从而隐藏鼠标的子模块；解锁模块包括一用于关闭第一定时器，恢复鼠标位置的子模块。

9. 根据权利要求1所述的实时锁屏系统，其特征在于所述密码认证模块用于：判断一级密码是否正确，如果一级密码正确，则判断二级密码是否正确；如果二级密码正确，则判断下一级密码是否正确，以此类推，如果前面各级密码均正确，则判断最后一级密码是否正确；如果最后一级密码也正确，则由解锁模块解除锁屏操作；如果各级密码有一级错误，则弹出警告，警告后加锁模块进入锁屏操作。

10. 根据权利要求1所述的实时锁屏系统，其特征在于所述密码设置模块用于：设置一级密码；用户确定设置一级密码之后，则设置二级密码；用户确定设置二级密码之后，则设置下一级密码；以此类推；用户确定设置四级密码之后，则设置最后一级密码；用户确定设置最后一级密码之后，加密各级密码，将加密之后的密码保存到配置文件；如果多级密码认证失败，或者用户取消任何一级密码设置，则取消整个密码设置操作。
实时锁屏系统

技术领域
[0001] 本发明涉及一种 Windows 下的锁屏系统，特别涉及一种传媒等相关的领域中关于实时保护媒体播放机的安全运行的系统。

背景技术
[0002] 目前，Windows 操作系统被广泛使用，其便利性不言而喻，但是其中实时运行的应用程序乃至整个操作系统的安全性问题也是非常重要。例如，在传媒等相关领域，连接显示终端（液晶显示屏，LED 显示屏等）的媒体播放机非常普遍，这种主机实时运行着媒体节目播放软件，在安排好媒体节目之后，即可 24 小时不间断自动运行，其无人值守的状态下，非专业人员的操作或者恶意操作就会导致不良后果，如果媒体文件被替换更改，使得显示终端出现一些违法的内容，就会造成恶劣的社会影响和难以估计的损失，由此，应用程序实时运行的复杂性问题可见一斑。为了避免类似情况的发生，采取一定的方法来保护操作系统的安全运行显得非常重要。
[0003] 目前保护操作系统安全运行采用的方法主要有以下两种：
[0004] 1. 在实时运行的应用程序中嵌入锁定模块，直接锁定该应用程序，防止程序本身的安全性。这种方法显然安全性比较低，无法保护指定的应用程序以外的任何东西，另外，内嵌模块的方式需要对实时程序进行源代码级别的修改，这会在很大程度上提高实时程序的复杂度，从而导致其运行时的不稳定性，增加了开发和维护的成本。
[0005] 2. 利用一个全屏的窗口覆盖原桌面的一切，但是未阻断鼠标和键盘消息。这种方法在保护实时程序时过于彻底，由于全屏的窗口位于最顶层，使得受保护的实时程序（如媒体播放器）处于不可见状态，这也使得实时程序处于过保护状态，失去了正常的显示功能。另外，这种方法在保护操作系统时又显得力有未逮，由于键盘消息未被阻断，一些组合键操作即可使操作系统失去保护。

发明内容
[0006] 本发明要解决的技术问题是提供一种安全性高，运行稳定性好，开发和维护成本低，并且不妨碍应用程序本身正常功能的锁屏系统。
[0007] 为了解决上述技术问题，本发明的实时锁屏系统包括自动运行模块，密码初始化模块，加锁模块，消息阻断模块，密码认证模块，解锁模块；所述自动运行模块用于使锁屏系统在启动后自动运行；密码初始化模块用于读取配置文件中加密的用户密码，解密后对用户密码进行初始化；加锁模块包括锁屏模块和安装鼠标键盘钩子模块；消息阻断模块利用鼠标键盘钩子阻断鼠标和键盘消息，并且判断用户输入的按键是否与鼠标键盘钩子中的解锁按键码相同；若相同则解锁键盘，允许输入用户密码，否则阻断鼠标和键盘消息；密码认证模块用于判断用户输入的密码是否与用户密码相同，否则由解锁模块解除锁屏操作，卸载鼠标键盘钩子。
[0008] 本发明可适用于待保护的 Windows 操作系统，其随操作系统启动，利用锁屏模块
进行锁屏操作，利用鼠标键盘键子阻断一切鼠标键盘消息，包括复杂的组合键操作。用户必须按特定解锁键并且通过密码认证才能解锁屏幕。防止非法用户的误操作和恶意操作，提高了系统的安全性；同时解锁按键和密码认证提高了锁屏系统本身的生存能力。锁屏模块与鼠标键盘键子提供双重防护，不留下任何安全死角。另外，本发明独立于操作系统中其他应用程序，不影响实时运行应用程序的正常功能。本发明安全度高，运行稳定性好，开发和维护成本低。

【0009】所述密码初始化模块还用于初始化超级密码。

【0110】本发明还包括托盘服务模块和密码设置模块；所述托盘服务模块用于解锁状态下等待用户的加锁、用户密码设置和退出操作；密码设置模块用于重置用户密码，并将用户密码加密后保存到配置文件。

【0111】本发明利用托盘服务模块和密码设置模块使用户能够在解锁状态下对系统进行加锁、密码设置和退出操作，托盘界面简洁，操作方便，密码设置便于用户管理密码，更加人性化，也更安全。

【0112】所述锁屏模块包括一用于最大化程序主窗口，使其置顶，并且透明的子模块；解锁模块包括一用于最小化程序主窗口的子模块。

【0113】所述锁屏模块包括一用于隐藏，锁定任务栏的子模块；解锁模块包括一用于任务栏解锁的子模块。

【0114】所述锁屏模块包括一用于任务管理器锁定的子模块；解锁模块包括一用于任务管理器解锁的子模块。

【0115】所述任务管理器锁定子模块，用于修改注册表，禁止任务管理器；或利用第一定时器定时关闭任务管理器窗口；或修改注册表，禁止任务管理器的同时打开第一定时器，随之关闭任务管理器窗口；任务管理器解锁子模块，用于修改注册表，打开任务管理器；或关闭第一定时器，解除任务管理器的锁定；或修改注册表，打开任务管理器，同时关闭第一定时器，解除任务管理器的锁定。

【0116】所述锁屏模块包括一用于开启第二定时器，将鼠标位置设定到屏幕范围之外，从而隐藏鼠标的子模块；解锁模块包括一用于关闭第二定时器，恢复鼠标位置的子模块。

【0117】所述密码认证模块用于：判断一级密码是否正确，如果一级密码正确，则判断二级密码是否正确，如果二级密码正确，则判断下一级密码是否正确，以此类推，如果前面各级密码均正确，则判断最后一级密码是否正确，如果最后一级密码也正确，则由解锁模块解除锁屏操作，如果各级密码有二级错误，则弹出警告，警告后加锁模块进行锁屏操作。

【0118】所述密码设置模块用于；设置一级密码；用户确定设置一级密码之后，则设置二级密码；用户确定设置二级密码之后，则设置下一级密码；以此类推；用户确定设置前面各级密码之后，则设置下一级密码；用户确定设置最后密码之后，加密各级密码，将加密之后的密码保存到配置文件；如果多级密码认证失败，或者用户取消任何一级密码设置，则取消整个密码设置操作。

【0119】本发明提供了多级密码认证，多级密码设置和密码加密保护等功能，进一步提高了操作系统的安全性。

附图说明
具体实施方式

如图1所示，本发明的实时锁屏系统包括自动运行模块101，密码初始化模块102，加锁模块103，消息阻断模块104，密码认证模块105，解锁模块106，托盘伺服模块107和密码设置模块108。

0028 自动运行模块101用于使锁屏系统随操作系统自动运行。
0029 密码初始化模块102用于读取配置文件中的加密密码，解密后初始化。
0030 加锁模块103包括锁屏模块和安装鼠标键盘键子模块，用于真正的锁屏操作。
0031 锁屏模块可以使用下述子模块中的一个或多个进行加锁操作：
0032 用于最大化程序主窗口，使其置顶，并且透明的子模块；
0033 用于隐藏，锁定任务栏的子模块；
0034 用于任务管理器锁定的子模块：用于修改注册表，禁止任务管理器；或利用第一定时器随时关闭任务管理器窗口；或修改注册表，禁止任务管理器的定时同时打开第一定时器，
0035 随时关闭任务管理器窗口。
0036 用于开启第二定时器，将鼠标位置设定到屏幕范围之外，从而隐藏鼠标的子模块。
0037 消息阻断模块利用鼠标键盘键子阻断鼠标和键盘消息，并且判断用户输入的按键是否与鼠标键盘键子中的解锁按键码相同，若相同则解锁键盘，允许输入用户密码，否则阻断鼠标和键盘消息。
0038 密码认证模块105用于认证用户身份，判断是否解除锁屏操作；判断一级密码是否正确，如果一级密码正确，则判断二级密码是否正确；如果二级密码正确，则判断下一级密码是否正确，以此类推，如果前面各级密码均正确，则判断最后一级密码是否正确；如果最后一级密码也正确，则由解锁模块解除锁屏操作，如果各级密码有一级错误，则弹出警告，警告后加锁模块进行锁屏操作。
0039 解锁模块106用于解除锁屏操作，卸载鼠标键盘键子。
0040 对应于加锁模块，解锁模块106可以利用下述一个或多个子模块解除锁屏操作：
0041 用于最小化程序主窗口的子模块；
0042 用于任务管理器解锁的子模块：用于修改注册表，打开任务管理器；关闭或第一定时器，解除任务管理器的锁定；或修改注册表，打开任务管理器，同时关闭第一定时器，解除任务管理器的锁定。
0043 用于关闭第二定时器，恢复鼠标位置的子模块。
0044 所述托盘伺服模块107用于锁屏状态下等待用户的加锁、用户密码设置和退出操
所述密码设置模块108用于重置用户密码，并将用户密码加密后保存到配置文件。

如图2所示，实现实时锁屏的主程序包括如下步骤：

步骤201：开始运行程序，可以是用户手动运行，也可以是系统自动运行；
步骤202：初始化托盘，这是主程序的UI；
步骤203：初始化超级密码以防止用户忘记密码；
步骤204：从配置文件中读取加密的多级用户密码，解密后初始化多级用户密码；
步骤205：调用加锁操作子程序，进行锁屏操作并安装鼠标键盘钩子；
步骤206：利用鼠标键盘钩子截取用户按键信息，判断用户输入的按键是否与鼠标键盘钩子中的解锁按键码相同，例如F2；如果不是解锁按键，则继续判断用户输入；
步骤207：如果用户输入的按键是解锁按键，则解锁键盘，使用户可以输入密码；
步骤208：进行多级密码认证；
步骤209：如果多级密码认证失败，则加锁键盘，继续判断用户输入；
步骤210：如果多级密码认证成功，则进行解锁操作；
步骤211：解锁之后，用户即可用托盘进行后续操作；
步骤212：用户可以用托盘进行加锁操作；
步骤213：用户可以用托盘进行设置多级密码操作；
步骤214：用户可以用托盘执行退出操作；
步骤215：退出需要多级密码认证，如果多级密码认证失败，则无法退出；
步骤216：如果多级密码认证成功，则程序结束。

如图3所示，加锁操作子程序包括下述步骤：
步骤301：由程序主线程或其它线程调用开始运行
步骤302：首先最大化程序主窗口，使其置顶，并且透明；
步骤303：隐藏，锁定任务栏；
步骤304：修改注册表，禁止任务管理器，同时打开第一定时器，随时关闭任务管理器窗口，从而达到锁定任务管理器的目的；
步骤305：开启第一定时器，将鼠标位置设定到屏幕范围之外，从而达到隐藏鼠标的作用；
步骤306：安装鼠标键盘钩子，截获所有鼠标键盘消息；
步骤307：完成加锁操作，返回到主程序流程。

如图4所示，解锁操作子程序包括下述步骤：
步骤401：由程序主线程或其它线程调用开始运行；
步骤402：卸载鼠标键盘钩子；
步骤403：关闭第二定时器，恢复鼠标位置；
步骤404：修改注册表，打开任务管理器的禁止功能，关闭第一定时器，解除任务管理器的锁定；
步骤405：解锁任务栏；
步骤406：主窗口最小化；
步骤 407：完成解锁操作，返回到主流程。

步骤 501：由程序主流程或其它子流程间调用开始运行。

步骤 502：判断一级密码是否正确。

步骤 503：如果一级密码正确，则判断二级密码是否正确。

步骤 504：如果二级密码正确，则判断下一级密码。

步骤 505：前面各级密码均正确，则判断最后一级密码。

步骤 506：如果最后级密码也正确，则返回 true，进行解锁操作。

步骤 507：如果各级密码有一级错误，则弹出警告。

步骤 508：警告后返回 false，加锁键盘，继续判断用户输入。

步骤 509：完成多级密码认证，返回到主流程。

如图 6 所示，设置密码子流程包括下述步骤：

步骤 601：由程序主流程或其它子流程间调用开始运行。

步骤 602：进行多级密码认证。

步骤 603：多级密码认证成功，则设置一级密码。

步骤 604：确定设置一级密码之后，则设置二级密码。

步骤 605：确定设置二级密码之后，则设置下一级密码。

步骤 606：确定设置前面各级密码之后，则设置最后一级密码。

步骤 607：确定设置最后一级密码之后，则加锁各解密。

步骤 608：将加锁之后的用户密码保存到配置文件。

步骤 609：如果多级密码认证失败，或者用户取消任何一级密码设置，则取消整个设置操作。

步骤 610：完成多级密码设置，返回到主流程。

下面具体说明本发明的实现方案：

本发明提出的实时锁屏系统在 Windows 系统下使用 MS Visual Studio 来实现。

步骤 1，首先创建一个动态链接库，在其中实现钩子的功能。

步骤 2，设置进程间共享的全局变量，全局窗口句柄，全局鼠标钩子句柄，全局键盘钩子句柄，以及全局组合键钩子句柄。

步骤 3，实现鼠标钩子处理函数，屏蔽所有的鼠标消息。

步骤 4，实现键盘钩子处理函数，屏蔽除解锁按键之外的所有键盘消息。

步骤 5，实现组合键钩子处理函数，屏蔽常用的组合按键消息。

步骤 6，实现安装钩子接口，安装鼠标钩子，键盘钩子和组合键钩子。

步骤 7，实现卸载钩子接口，卸载鼠标钩子，键盘钩子和组合键钩子。

步骤 8，实现安装键盘钩子和卸载键盘钩子的接口。

步骤 9，编译生成 dll 和 lib 文件。

步骤 10，创建一个基于对话框的 MFC 工程，作为锁屏系统主程序。

步骤 11，将步骤 9 生成的 dll 和 lib 复制到对话框工程目录，并且在工程属性中设置好 lib 库依赖。

步骤 12，增加输入密码对话框，设置密码对话框，以及警告信息对话框资源。
步骤 13，实现输入密码对话框和设置密码对话框的获得密码接口以及确定按钮消息处理函数。

步骤 14，实现警告消息对话框的设置消息接口。

步骤 15，实现密码类，在其中实现密码设置和密码判断接口。

步骤 16，实现密码管理类，在其中实现添加、删除以及保存和加载接口。

步骤 17，在主程序对话框类中，实现托盘初始化，托盘状态改变消息处理，托盘弹出以及托盘退出以及托盘回调相关接口。

步骤 18，在主程序对话框类中，实现初始化密码接口，在其中加载和初始化普通密码和初始化超级密码，实现密码保存和加载接口，实现多级密码认证的函数以及多级密码设置接口。

步骤 19，实现主窗口最大化，透明和置顶操作接口。

步骤 20，实现主窗口最小化接口。

步骤 21，分别实现锁定任务栏和解锁任务栏接口。

步骤 22，分别实现锁定任务管理器和解锁任务管理器接口。

步骤 23，分别实现安装钩子和卸载钩子接口。

步骤 24，分别实现锁定鼠标和解锁鼠标接口。

步骤 25，实现定时器处理函数。

步骤 26，实现解锁键盘和加载键盘接口。

步骤 27，实现加载操作接口。

步骤 28，实现解锁操作接口，此功能由前述的钩子来触发。

步骤 29，实现主程序退出接口，完成系统解锁和资源释放。

步骤 30，在主对话框的初始化函数中，加入各个初始化接口和加载操作接口。

步骤 31，在托盘的消息处理函数中，分别加入设置密码，主程序退出和加载操作接口。

步骤 32，编译生成 exe 文件。

以上所述，仅是本发明的较佳实施例，不应被视为是对本发明范围的限制，本发明要求保护的范围以权利要求为准。
图6