[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G11C 16/22 (2006.01)
G11C 11/412 (2006.01)

[12] 发明专利说明书

专利号 ZL 02825751.0

[45] 授权公告日 2007 年 7 月 18 日

[11] 授权公告号 CN 1327357C

[22] 申请日 2002.10.4 [21] 申请号 02825751.0
[30] 优先权
[32] 2002.7.31 [33] SG [31] PCT/SG02/00171
[86] 国际申请 PCT/SG2002/000227 2002.10.4
[87] 国际公布 WO2004/015515 英 2004.2.19
[85] 进入国家阶段日期 2004.6.21
[73] 专利权人 特科 2000 国际有限公司
地址 新加坡新加坡
[72] 发明人 黄敬弦 林利泉 符廷彬 陈亨利
[56] 参考文献
WO95016238A 1995.6.15
审查员 张 妍

[74] 专利代理机构 北京纪凯知识产权代理有限公司
代理人 戈 泊 程 伟

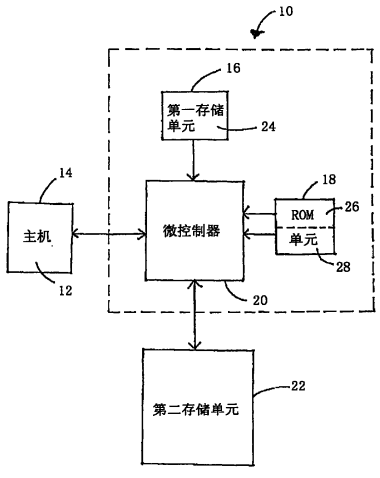
权利要求书 3 页 说明书 9 页 附图 7 页

[54] 发明名称

用于验证的系统和方法

[57] 摘要

提供校验密码的验证系统。 验证系统包括存储验证序列的第一存储单元和在其上编程验证算法的只读存储单元。 微控制器连接到第一存储单元、只读存储单元和万维网服务器上。 微控制器接收密码并执行验证算法以便通过验证序列校验密码。 第二存储单元连接到微控制器以便存储来自万维网服务器的数据。 只有当已经校验过密码后，才由微控制器允许存取第二存储单元。



1．一种校验密码的验证系统，该系统用于连接到主机与主机进行通信，并包括：

存储验证序列的第一存储单元；

存储验证算法的只读存储器；

连接到所述第一存储单元、所述只读存储器和万维网服务器的微控制器，其中，所述微控制器接收所述密码和执行所述验证算法，以及其中所述验证算法通过所述验证序列校验所述密码；以及

连接到所述微控制器的第二存储单元，存储来自所述万维网服务器的数据，以及其中，只有当校验过所述密码后，才由所述微控制器允许存取所述第二存储单元，

其中该系统用于从万维网服务器经过主机接收加密格式的数据，并在主机使用数据之前解密该数据。

2．如权利要求 1 所述的验证系统，由所述微控制器从所述主机接收所述密码。

3．如权利要求 2 所述的验证系统，其特征在于，所述只读存储器进一步包括关机算法以便在由所述微控制器接收多个不正确密码后，停止所述主机和所述验证系统。

4．如权利要求 2 所述的验证系统，其特征在于，由所述主机从所述万维网服务器接收所述密码。

5．如权利要求 2 所述的验证系统，其特征在于，在由所述微控制器中的固件和硬件组成的一个组上硬编码所述验证算法。

6．如权利要求 5 所述的验证系统，其特征在于，所述第二存储单元是移动存储设备。

7. 如权利要求 6 所述的验证系统，其特征在于，所述第二存储单元使用闪速存储器。

8. 如权利要求 2 所述的验证系统，其特征在于，在单个半导体芯片上实现所述微控制器和所述只读存储单元。

9. 如权利要求 8 所述的验证系统，其特征在于，所述第一存储单元和所述只读存储单元合并到所述微控制器中。

10. 如权利要求 1 所述的验证系统，进一步包括连接在所述微控制器和所述第二存储单元间的编码器，其中，所述编码器加密将写到所述第二存储单元上的数据。

11. 如权利要求 10 所述的验证系统，进一步包括连接在所述微控制器和所述第二存储单元间的解码器，其中，所述解码器解密将从所述第二存储单元读取的数据。

12. 如权利要求 11 所述的验证系统，其特征在于，散列编码存储在所述第二存储单元中的数据。

13. 如权利要求 12 所述的验证系统，其特征在于，加密所述验证序列。

14. 如权利要求 12 所述的验证系统，其特征在于，散列编码所述验证序列。

15. 如权利要求 1 所述的验证系统，其特征在于，所述第一存储单元位于所述只读存储单元中，以及其中，将所述验证序列散列编码到所述第一存储单元中。

16. 如权利要求 15 所述的验证系统，其特征在于，所述第二存储

区进一步包括公用存储区和专用存储区。

17. 如权利要求 16 所述的验证系统，其特征在于，所述第一存储单元位于所述第二存储区的所述专用存储区中。

18. 一种用于验证密码的方法，包括：

将验证系统连接到主机用于与主机通信；

该系统接收所述密码；

该系统从所述万维网服务器经过主机接收加密格式的数据，其中，所述数据存储在该系统的存储单元中；

该系统提供验证序列；

该系统执行验证算法以便通过所述验证序列校验所述密码，其中所述验证算法存储在该系统的只读存储单元上；

只有当校验所述密码后，该系统才允许存取所述存储单元上的所述数据；以及

该系统在主机使用该数据之前解密该数据。

19. 如权利要求 18 所述的用于验证密码的方法，其特征在于，从所述万维网服务器接收所述密码。

20. 如权利要求 19 所述的用于验证密码的方法，其特征在于，由用户输入所述密码。

用于验证的系统和方法

技术领域

本发明通常涉及数字和软件盗版。更具体地说，本发明涉及用于验证以便防止数字系统中盗版的系统和方法。

背景技术

软件和其他数字介质的盗版和非法复制已经变得极其普遍，通常导致全世界的媒介和软件拥有者数十亿的利润损失。这一问题随着更快和更有技术的先进计算机的到来、廉价大容量存储器(即，CDs，DVDs)的开发，以及帮助数字盗版的各个方面的复制设备诸如CD刻录机变得更复杂。

每个技术成就表面上看来产生非法复制属于另一个的知识产权的新的和更好的方法。数字盗版的例子包括：复制专有软件以便出售给他人、在几个不同系统上安装单一专有软件包、将专有软件的副本放在Internet上或甚至从Internet下载版权图象。

尽管在已经合法购买软件的许多终端用户中，数字盗版是相当普遍，大规模盗版通常发生在再销售商层。例如，再销售商可以复制和将软件程序、数字音频文件或数字视频文件的多个副本分发给不同用户。这些仿造版本有时被传递到未怀疑的用户。已知硬件销售商使用单个软件包预载不同系统。在这些例子中，未向用户提供原始手册、磁盘和/或光盘（CDs）或简单地提供其盗版副本。

已经设计了防止数字盗版的蔓延问题的许多方法。一个方法是使用试用版软件（trialware）来限制使用软件产品。可以通过将截止日期或使用次数编程为软件程序来实现试用版软件。这种方案分别将软件产品的使用限制到特定持续时间或试用时间（trial time），在此之后，不再运行受保护的应用程序。然后迫使用户购买全版产品或完全退出使用它。

硬件密钥是另一种防盗版设备，通常用来防止非法使用软件。硬

件密钥是插入所选定的计算机端口的设备。只要执行软件，那么它用与检测其他硬件设备（诸如打印机、监视器或鼠标）类似的方式，检测硬件密钥的存在。编程软件以便它仅当连接适当的硬件密钥时才操作，防止非法使用软件。由于分配终端用户的硬件密钥的数量对应于所购买的客户访问许可证（seat license）的数量，当安装在没有必要硬件密钥的另一系统上时，该软件将不起作用。

另一通用的防盗版技术是要求在安装软件之前，输入由软件公司提供的某一注册密钥。传统上，仅与原始软件包一起给予注册密钥，尽管一些被电子地发行。不幸地是，无法防止注册密钥的持有者将软件安装在几个系统上。另外，许多电子注册密钥基于用户的个人信息（即，诸如用户名），因此，一些黑客已经开发了计算用于任意名的注册密钥的程序。

不幸地是，通过使用注册密钥，黑客很容易避开所有上述防盗版系统（以及许多其他系统）。对抗这些防盗版技术的通用方法是将应用编程接口（API）的编码反汇编成汇编语言，此后，将汇编语言反编译成编程语言。通过从程序流获得的知识，黑客能容易重写程序或在程序本身内设置某些条件，以致回避所有防盗版验证算法。

由上文看来，非常需要具有不能由计算机黑客或其他数字盗版容易重编程或回避的防盗版系统。还需要具有能与现有大容量存储设备结合的防盗版系统。

发明内容

本发明通过提供用于验证的系统和方法来满足这些需要。应意识到本发明能用多种方法实现，包括过程、装置、系统、设备或方法。下面描述本发明的几个发明创造的实施例。

在本发明的一个实施例中，提供校验密码的验证系统。验证系统包括存储验证序列的第一存储单元和在其上编程验证算法的只读存储器。最好加密或散列该编码验证序列。微控制器连接到第一存储单元、只读存储器和万维网服务器。连接到微控制器的第二存储单元存储来自万维网服务器的数据。微控制器接收密码并执行验证算法以便通过验证序列校验密码。只有当校验过密码后，才由微控制器允许存取第

二存储单元。最好加密来自万维网服务器将存储在第二存储单元上的数据。另外，可以散列编码数据。

只读存储单元最好包括关机算法以便当由微控制器接收一系列不正确密码时，停止主机和验证系统。最好在单个芯片上实现第一存储单元、微控制器、只读存储单元和第二存储单元。另外，最好使第一存储单元和只读存储单元合并到微控制器上。

在本发明的优选实施例中，在固件或硬件上实现验证算法。第一存储单元最好位于只读存储单元上以及验证序列最好硬编码成验证算法。另外，第一存储单元可以位于第二存储设备中。

在本发明的另一实施例中，提供用于验证密码的方法。该方法通过提供验证序列和接收密码开始。执行存储在只读存储单元上的验证算法以便通过验证序列校验密码。只有当校验密码后，才允许存取万维网服务器或存储单元上的数据。如果接收多个不正确密码后，最好停止整个系统。最好加密或解密来自万维网服务器并且将存储在存储单元中的数据。另外，散列编码数据。

从下述结合附图、通过举例示例说明本发明的原理的详细的描述，本发明的其他方面和优点将变得显而易见。

附图说明

通过下述结合附图的详细描述，很容易理解本发明。为便于这一描述，相同的标记表示相同的结构元件。

图 1 示例说明根据本发明的一个实施例，校验来自主机的密码的验证系统的示意图；

图 2 示例说明根据本发明的另一实施例，校验来自主机的密码的验证系统的示意图；

图 3 示例说明根据本发明的另一实施例，校验来自主机的密码的验证系统的示意图；

图 4 示例说明根据本发明的另一实施例，校验来自主机的密码的验证系统的示意图；

图 5 示例说明根据本发明的一个实施例，由主机验证密码的方法；

图 6 示例说明根据本发明的另一实施例，使用防盗版文件管理器

的计算机系统的示意图；

图 7 示例说明根据本发明的另一实施例，用于从万维网服务器接收数据的验证系统的示意图。

具体实施方式

提供用于在数字系统中验证的系统和方法。在下述描述中，阐述许多具体的细节以便提供本发明的全面理解。然而，将理解到对本领域的技术人员来说，在没有一些或全部这些具体细节的情况下，也可以实施本发明。在其他例子中，未详细地描述非常公知的过程操作以便不必要地使本发明不清楚。

图 1 示例说明根据本发明的一个实施例，校验来自主机 14 的密码 12 的验证系统 10。验证系统 10 包括第一存储单元 16、只读存储器（ROM）单元 18 和微控制器 20。微控制器 20 连接到主机 14、第一存储单元 16、ROM 单元 18 和第二存储单元 22。微控制器 20 最好通过通用串行总线（USB）控制器连接到主机 14。

在本发明的另一实施例中，ROM 单元 18 可以形成为微控制器 20 的一部分。此外，第一存储单元 16 和第二存储单元 22 可以是多个大容量存储设备的一个，包括硬驱动器、软盘或移动闪速存储设备，诸如由 Trek2000 制造的 ThumbDrive。另外，两个存储单元可以用在一个物理结构中以便形成单一大容量存储设备。大容量存储设备也可以与微控制器 20 放在一起以便形成单一芯片。

第一存储单元 16 存储验证序列 24，其用来校验密码 12。验证密码 12 的验证算法 26 和验证序列 24 一起被编码在 ROM 单元 18 上。另外，ROM 单元 18 最好包括关机算法（shutdown algorithm）28。因为这些算法和其他数据是硬编码的，ROM 单元 18 的内容不能被再编译或再修改。在接收密码 12 后，微控制器 20 加载和执行验证算法 26 以便校验密码 12 和验证序列 24。只有当校验密码 12 后，才允许存取第二存储单元 22。

在从微控制器 20 接收询问后，可以由用户或主机 14 执行的软件程序输入密码 12。因为验证算法 26 被硬编码在 ROM 单元 18 上，复制或再编译和改变驻留在主机 14 上的软件程序不能破坏由本发明提供的

版权保护。对本领域的技术人员来说密码 12 可以是私有字符串、通信协议序列或仅授权用户所知的其他一些保密协议是显而易见的。另外，密码 12 和验证序列 24 可以通过使用用户的指纹、虹膜、脸或语音作为验证手段，形成为生物验证的一部分。

密码 12 还可以被编程到在主机 14 上运行的软件上以及仅可以由验证算法 26 识别，因此，对终端用户是未知的。如上所述，最好在硬件或固件（诸如 ROM 单元 18）上实现验证算法 26 以便其防篡改；即，验证算法 26 将极其难以逆操纵或抽取数据，因此极其难以回避。

关机算法 28 最好通过如果由微控制器 20 接收到一系列不正确密码，停止整个系统来实现以阻止蛮力攻击。验证系统程序员可以定义在系统关机前允许的不正确密码的最大次数。关机算法 28 还可以编程以便再也不接受达特定次数的密码输入。通过使用关机算法 28，由蛮力应用程序使用来识别密码 12 的试验和误差方法对黑客来说将变成缓慢的过程。因此，算法阻止潜在的黑客试图识别密码 12。

第二存储单元 22 用来存储主机 12 上的程序运行所需的程序和/或文件。这种文件的例子包括可执行程序（诸如软件安装程序）、数字音频文件、数字视频文件、图象文件、文本文件和库文件。微控制器 20 只有当由微控制器 20 接收到正确密码 12 后，才允许从主机 14 存取第二存储单元 22。

尽管在这一实施例中示例为单个实体，对本领域的技术人员来说可以用多个方法组合微控制器 20、第一存储单元 16、ROM 单元 18 和第二存储单元 22 应当是显而易见的。例如，可以在单个半导体芯片上实现微控制器 20、第一存储单元 16、ROM 单元 18 和第二存储单元 22。在另一实施例中，可以在与存储单元分开的芯片上实现微控制器 20 和 ROM 单元 18 。

因此，本发明具有很大的设计灵活性，可以根据用户需求容易改变。例如，一方面，使用多个芯片可以允许不同的卖方制造验证系统的不同部分。另一方面，将本发明制作在更少芯片（或单一芯片）上可以更廉价并提供更好的性能。另外，如果 ROM 单元 18 和微控制器 20 位于相同芯片上，更难以分开 ROM 以便读取存储在其上的数据。

图 2 示例说明根据本发明的另一实施例，校验来自主机 54 的密码

52 的验证系统 50。验证系统 50 包括第一存储单元 56、ROM 单元 58 和微控制器 60。微控制器 60 连接到主机 54、第一存储单元 56、ROM 单元 58 和编码器 62 上。编码器 62 进一步连接到第二存储单元 64。第一存储单元 54 存储用来校验密码 52 的验证序列 66。验证密码 52 的验证算法 68 被编程到 ROM 单元 58 上。ROM 单元 58 最好包括关机算法 70。

在接收密码 52 后，微控制器 60 加载和执行验证算法 68 以便通过验证序列 66 校验密码 52。只有当校验密码 52 后，才允许存取第二存储单元 64。如果由微控制器 60 接收一系列错误密码，关机算法 70 最好停止整个系统。验证系统程序员确定允许尝试不正确密码的最大次数。

首先分别由编码器解密或加密将从第二存储单元 64 上读取或写到其上的数据。可以由编码器 62 使用许多不同的加密方案，包括国际数据加密算法（IDEA）、数据加密标准（DES）加密、三重数据加密标准（3-DES）加密和高质量保密标准（PGP）。通过加密第二存储单元 64 的内容，即使黑客设法读取回避微控制器 60 的内容（例如通过使用探查），也不能懂得内容的含义。在已经验证过密码 52 后，可以使用解码器（未示出）来解密第二存储单元 64 的内容。

另外，存储在第二存储单元 64 中的数据可以由散列编码保护。另外，验证序列 66 最好也加密或散列以便防止黑客拆开验证序列 66。如果第一存储单元 56 位于第二存储单元 64 中，这可以不需要另外的编码器来实现。

图 3 示例说明根据本发明的另一实施例，校验来自主机 104 的密码 102 的验证系统 100 的示意图。验证系统 100 包括 ROM 单元 106 和微控制器 108。微控制器 108 连接到主机 104、ROM 单元 106 和编码器 110。编码器 110 进一步连接到存储单元 112。验证密码 102 的验证算法 114 被编程到 ROM 单元 106 上。校验密码 102 的验证序列 116 被硬编码到验证算法 114 上。ROM 单元 106 最好包括关机算法 118。

如在前实施例所述，在接收密码 102 后，微控制器 108 加载和执行验证算法 114 以便通过验证序列 116 校验密码 102。仅在校验密码 102 后，才允许存取存储单元 112。如果由微控制器 108 接收一系列不正确的密码后，最好使用关机算法 118 来停止整个系统。

通过直接将验证序列 116 硬编码到验证算法 114，可以在多个位置，修改验证序列 116 实质上变得更困难。为改变硬编码验证序列，不仅需要重新编译（如果使用编译语言），而且要求足够理解实现以便确保改变将不导致程序故障。这种措施使得黑客更难重新编程验证系统 100。

图 4 示例说明根据本发明的另一实施例，校验来自主机 154 的密码 152 的验证系统 150。验证系统 150 包括只读存储器（ROM）单元 156 和微控制器 158。微控制器 158 连接到主机 154、ROM 单元 156 和编码器 160。编码器 160 进一步连接到存储单元 162。首先分别由编码器 160 解密或加密从存储单元 162 读取或写到其上的的数据。另外，可以采用散列编码以便保护存储在存储单元 162 上的数据。

存储单元 162 由两种类型的数据存储区组成：公用存储区 164 和专用存储区 166。用来校验密码 152 的验证序列 168 存储在专用存储区 166 上。验证密码 152 的验证算法 170 被编程到 ROM 单元 156 上。ROM 单元 156 还包含关机算法 172。通过未宣告在存储单元 162 上可用的存储器大小，可以创建公用存储区 164 和专用存储区 166。

例如，具有从 000 至 1000 的物理地址的存储单元，只有当向主机 154 上的操作系统（OS）诸如 Windows 宣告物理地址 000 至 500，OS 将不知道存在物理地址 501 至 1000。在这种情况下，存储在物理地址 000 至 500 内的数据将可由任一用户存取。这一区称为公用存储区。相反地，未宣告的物理地址 501 至 1000 形成专用存储区，因为这些地址仅可用于微控制器 158 并仅能由授权用户或软件程序存取。

在未保密操作条件下，任一用户可以指示主机 154 来从公用存储区 164 上读取数据或将数据写到公用存储区 164 上。然而，如果用户希望存取公用存储区 166，用户或软件程序必须首先输入密码 152，然后将其发送到微控制器 158，用于验证。在接收密码 152 后，微控制器 158 执行验证算法 170 以便通过验证序列 168 校验密码 152。只有当校验密码 152 后，才允许存取专用存储区 166。如果由微控制器 158 接收到一系列不正确密码，关机算法 172 停止整个系统。

图 5 示例说明根据本发明的一个实施例，用于验证来自主机的密码的方法 200。首先在块 202 提供验证序列并最好存储在第一存储单元

中。同时在另一块 204 中提供存储在 ROM 单元中的验证算法。在从主机接收提示后，由用户或软件程序输入密码。然后，在块 206 由执行验证算法的微控制器接收密码以便在判定块 208 通过验证序列校验密码。

如果在判定块 208 中校验密码，在块 210 中将允许存取专用区，诸如上述实施例中的第二存储单元。然后，用户能读取或写入第二存储单元，最好是加密的。如果在判定块 208 中未校验密码，用户将不拒绝存取第二存储单元以及方法 200 将在块 212 中结束。另外，如果密码不正确，将给予用户另外的机会来输入正确密码。然而，如果由微控制器接收到一系列不正确密码，最好停止系统。

图 6 示例说明根据本发明的另一实施例，使用防盗版文件管理器 252 的计算机系统 250 的示意图。防盗版文件管理器 252 连接到防盗版验证机 254 和存储单元 256。防盗版管理器 252 应答来自多个软件程序 258 的请求，多个软件程序 258 请求来自防盗版验证机 254 的不同验证方案。由验证系统 260 保护存取存储单元 256。在这一示例性系统中，本发明的灵活性通过防盗版文件管理器 252 允许同时验证许多不同类型的软件程序。

图 7 示例说明根据本发明的另一实施例，用于从万维网服务器 302 接收数据的验证系统 300 的示意图。验证系统 300 连接到主机 304，主机 304 通常通过拨号或宽带连接连接到万维网服务器 302。主机 304 最好经 USB 连接器连接到验证系统 300。主机 304 的例子包括个人计算机（PC）、个人数字助理（PDA）、允许无线应用协议（允许 WAP）的移动电话和输入板。

为从万维网服务器 302 检索数据，通过验证系统 300 校验由主机 304 接收的密码。通常由用户或主机中的软件输入密码。如果由用户输入密码，还可以将验证系统配置成接受生物密码，诸如指纹或视网膜扫描。如果验证成功，验证系统 300 通过主机 304 发送存取万维网服务器 302 的请求。在接收到该请求后，万维网服务器 302 准许存取具有保密数据的网页。该数据可以以音乐文件或在线书或软件程序的形式。因为硬编码验证系统 300 中的验证算法，未授权用户将不能规避或改变验证系统 300 中的校验方案，因此，将不能存取万维网服务器

302 上的数据。

在本发明的另一实施例中，密码将嵌入将从 Internet 检索的数据中。主机 304 将用于数据的请求发送到万维网服务器 302。在接收到该请求后，万维网服务器 302 将嵌入所请求的数据中的密码发送到验证系统 300 用于校验。如果校验成功，在显示或执行它后，验证系统 300 允许主机 304 存取数据。在优选实施例中，加密来自万维网服务器 302 的数据。在用在主机 304 或存储在验证系统 300 之前，在验证系统 300 中执行数据的解密。

通过考虑本发明的说明和原理，对本领域的技术人员来说，本发明的其他实施例将是显而易见的。此外，某些术语用于描述清楚的目的，而不限制本发明。上述实施例和优选特征应当视为示例性的，由附加权利要求书限定本发明。

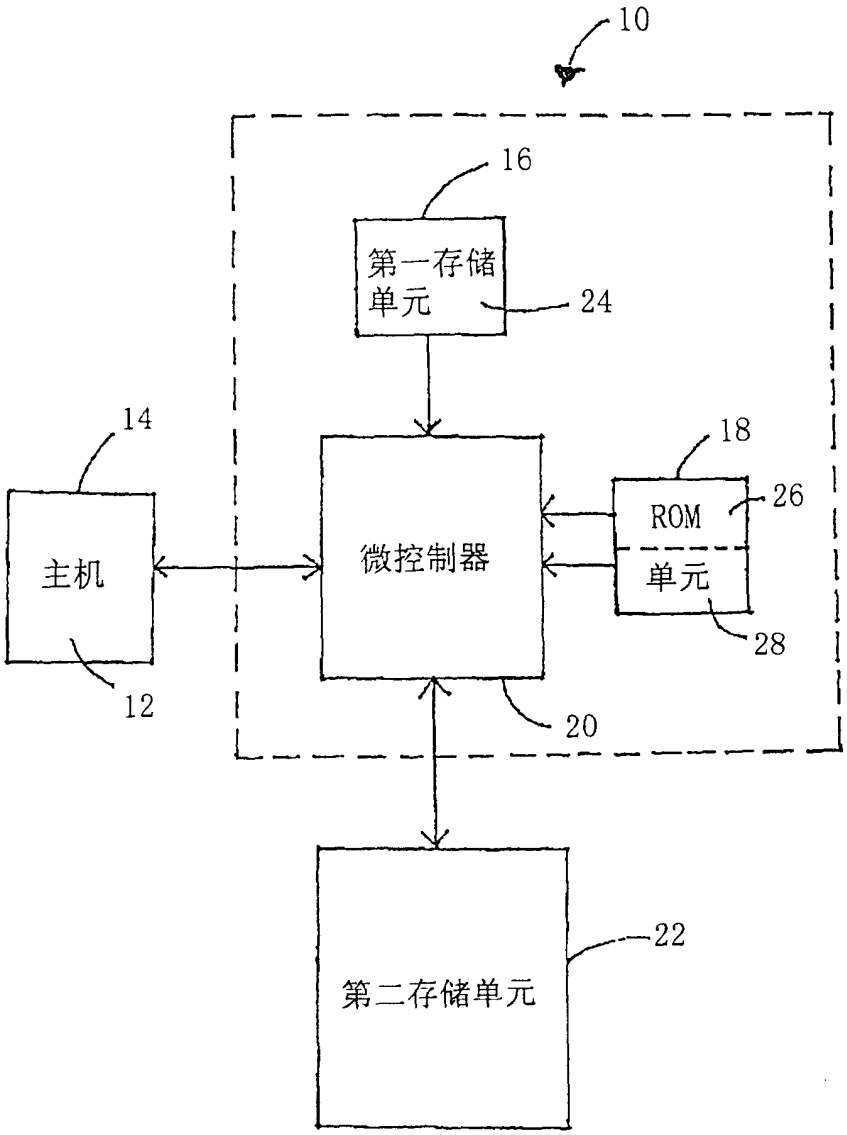


图1

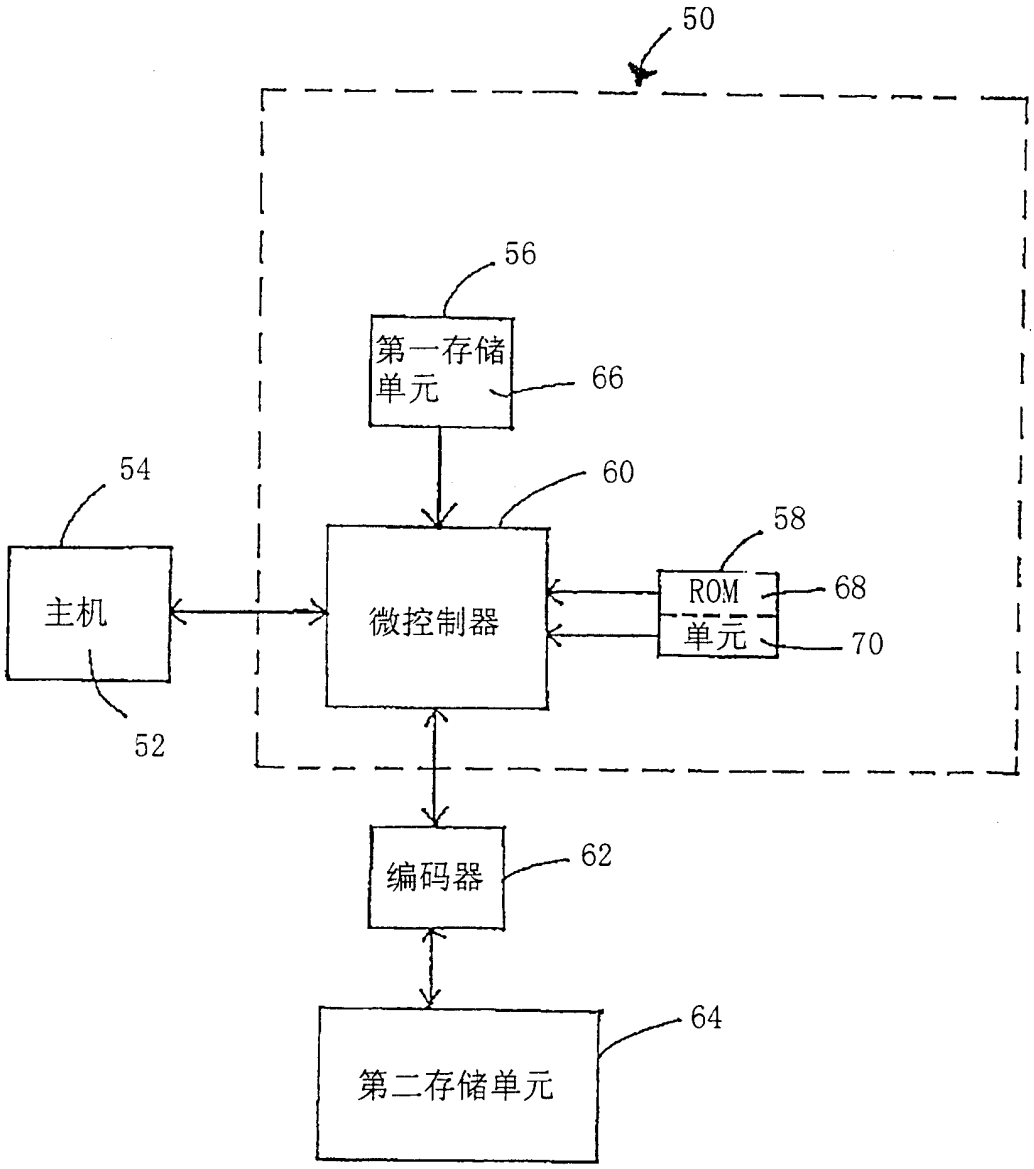


图2

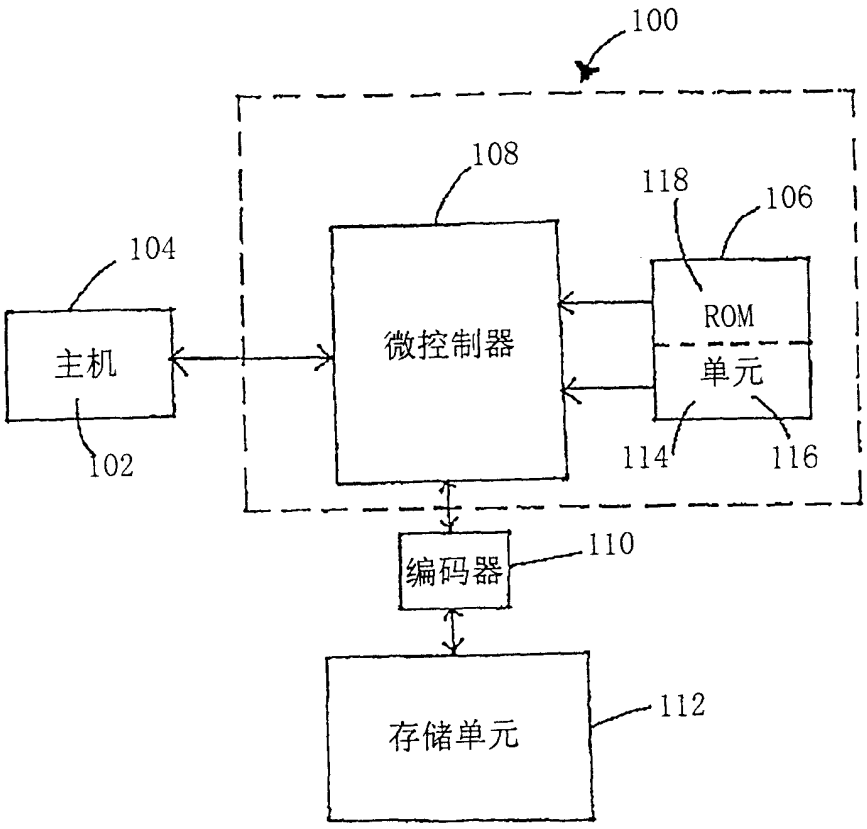


图3

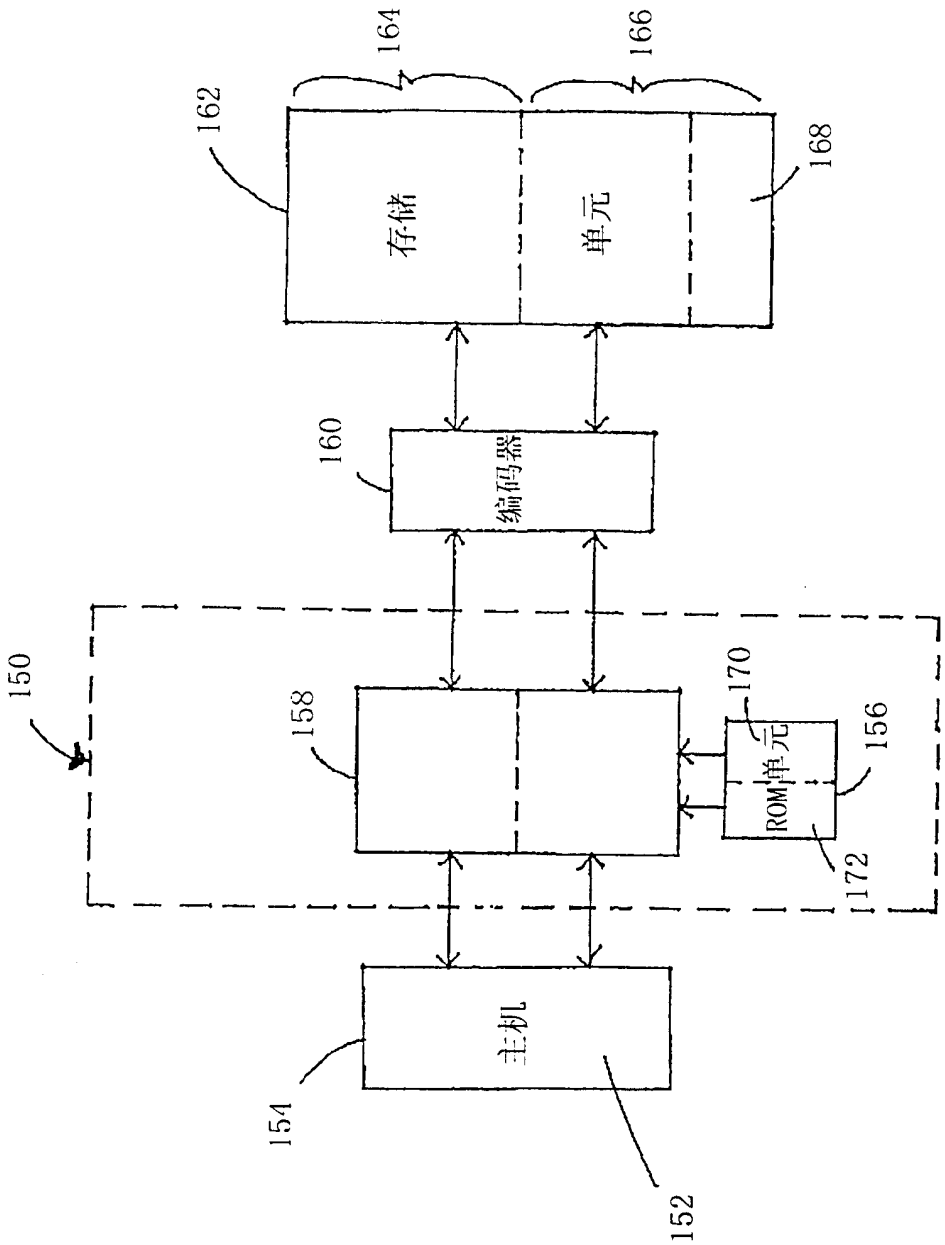

164
166
162
存储
单元
168
160
编码器
150
158
170
ROM单元
156
172
主机
154
152

图4

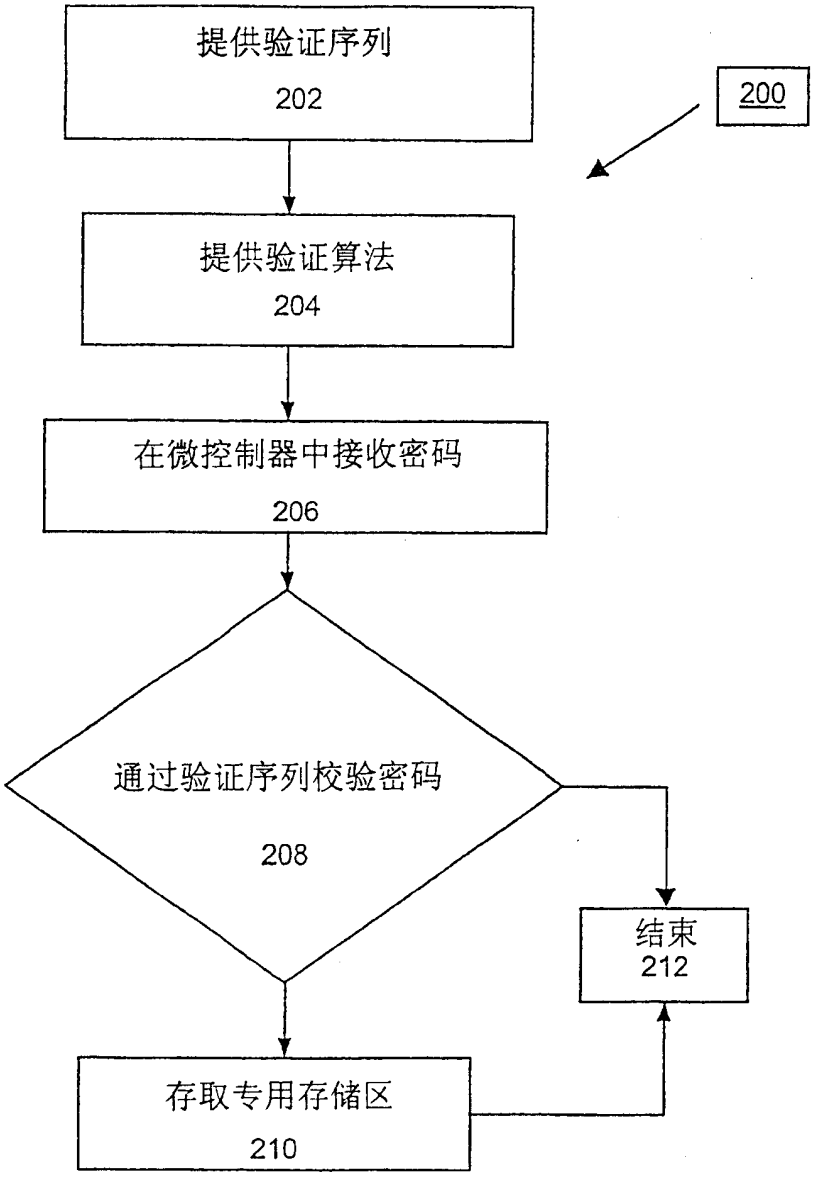

提供验证序列
202
200
提供验证算法
204
在微控制器中接收密码
206
通过验证序列校验密码
208
结束
212
存取专用存储区
210

图5

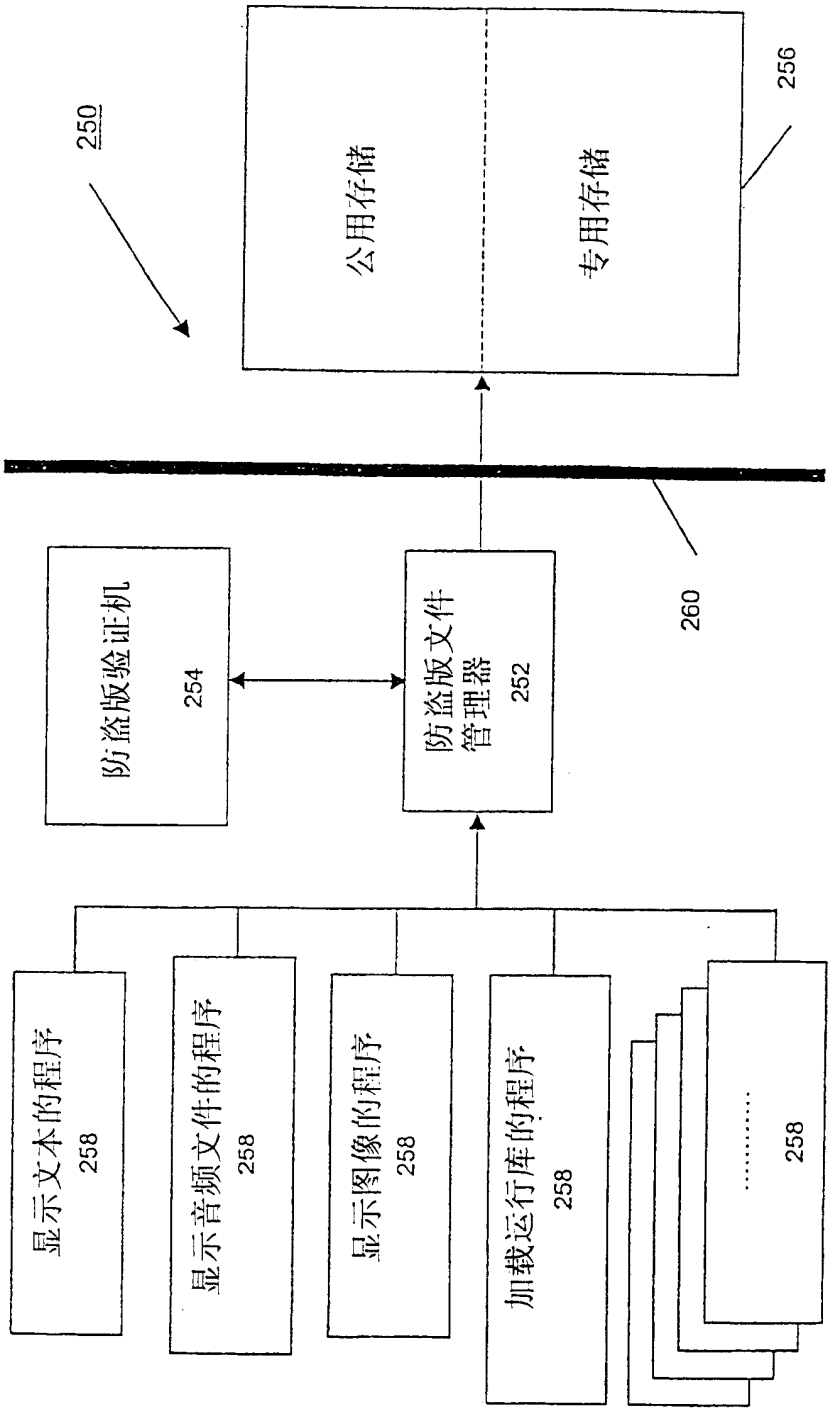

250
公用存储
专用存储
256
260
防盗版验证机
254
防盗版文件
管理器
252
显示文本的程序
258
显示音频文件的程序
258
显示图像的程序
258
加载运行库的程序
258
.....
258

图6

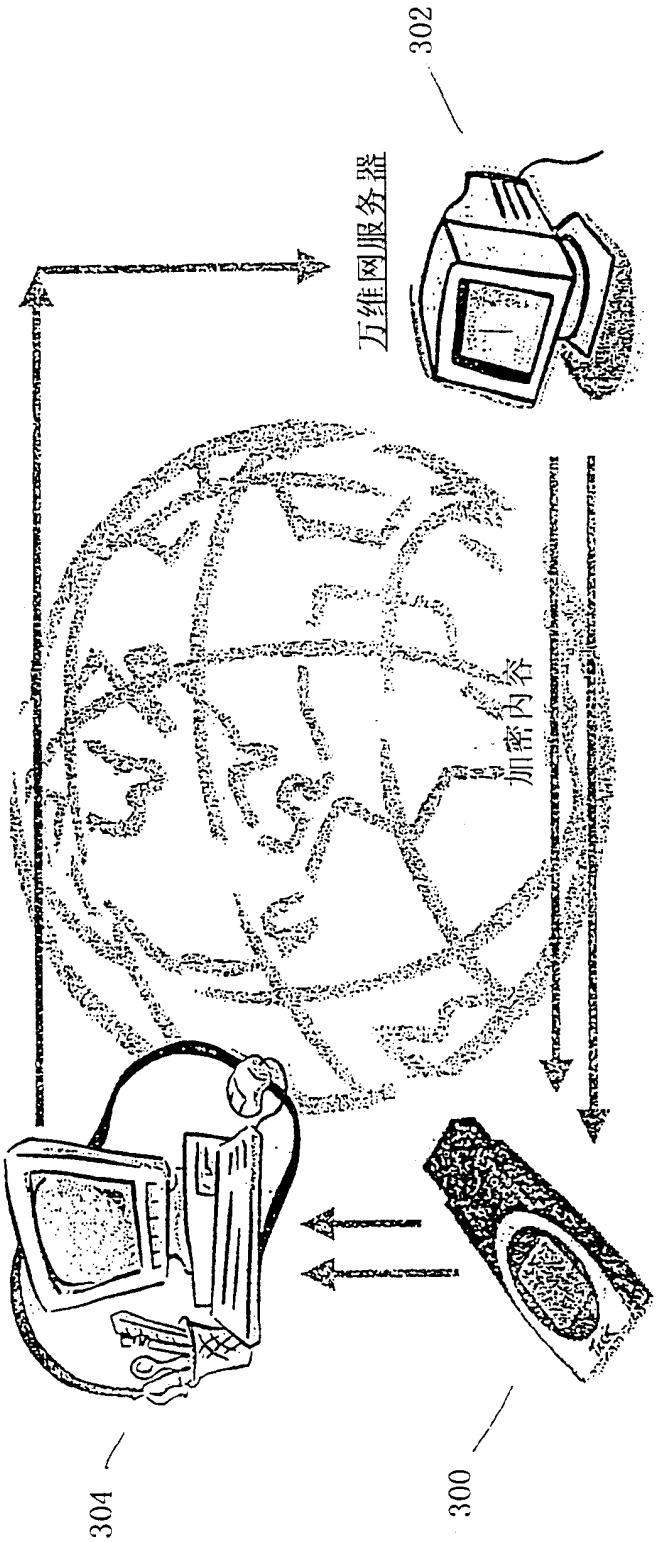


图7