(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 102799803 A
(43)申请公布日 2012.11.28

(21)申请号 201110359458.2

(22)申请日 2011.11.14

(30)优先权数据
13/115,457 2011.05.25 US

(71)申请人 英属开曼群岛商康帝国际科技股份有限公司
地址 英属西印度群岛开曼群岛

(72)发明人 林育中 苏志胜

(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 史新宏

(51)Int.Cl.
G06F 21/00(2006.01)

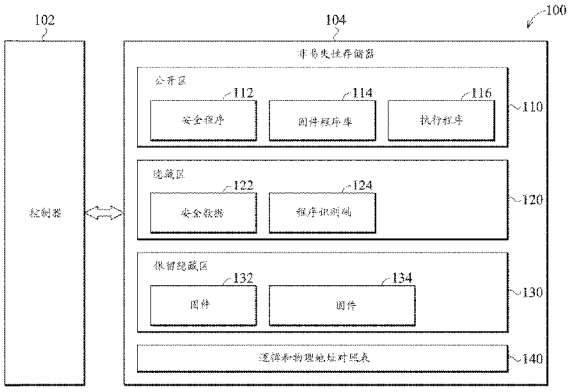
权利要求书 5 页 说明书 9 页 附图 13 页

(54)发明名称

安全可携式媒体以及管理安全可携式媒体的方法

(57)摘要

一种安全可携式媒体包括：一非易失性存储器，对应于一媒体识别码，且包括公开区、隐藏区、保留隐藏区以存取数据，其中撷取媒体识别码的第一固件和存取隐藏区的第二固件是储存于保留隐藏区中，媒体识别码被物理铭刻在非易失性存储器的半导体芯片上，且不会储存于正规存储器单元；一控制器，由一外部装置接收安全数据；以及一安全程序，储存于公开区，使用第一固件由非易失性存储器撷取媒体识别码，根据第一固件提供的媒体识别码产生一加密金钥，通过加密金钥加密安全数据以获得一加密安全数据，且使用第二固件将加密安全数据写入隐藏区中。



CN 102799803 A

1. 一种安全可携式媒体，包括：

一非易失性存储器，对应于一媒体识别码，且包括一公开区、一隐藏区、一保留隐藏区以储存数据，其中用以撷取上述媒体识别码的一第一固件，以及用以由上述隐藏区存取数据的一第二固件是储存于上述保留隐藏区中，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元；

一控制器，由一外部装置接收一安全数据；以及

一安全程序，储存于上述公开区，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码产生一加密金钥，通过上述加密金钥加密上述安全数据以获得一加密安全数据，以及使用上述第二固件将上述加密安全数据写入上述隐藏区中。

2. 根据权利要求 1 所述的安全可携式媒体，其中上述安全软件包括：

一固件链接库，启动上述第一固件由上述非易失性存储器撷取上述媒体识别码，以及启动上述第二固件将上述加密安全数据写入上述隐藏区中；

一金钥产生函式，根据上述第一固件提供的上述媒体识别码产生上述加密金钥；以及

一加密 / 解密函式，根据上述加密金钥加密上述安全数据以获得上述加密安全数据。

3. 根据权利要求 1 所述的安全可携式媒体，其中当由上述安全可携式媒体撷取上述安全数据时，上述安全程序由上述隐藏区读取上述加密安全数据，且由上述非易失性存储器撷取上述媒体识别码，根据由上述第一固件提供的上述媒体识别码产生一解密金钥，以及根据上述解密金钥解密上述加密安全数据以获得上述安全数据。

4. 根据权利要求 3 所述的安全可携式媒体，其中上述安全软件包括：

一固件链接库，启动上述第二固件由隐藏区读取上述加密安全数据，以及启动上述第一固件由上述非易失性存储器撷取上述媒体识别码；

一金钥产生函式，根据上述第一固件提供的上述媒体识别码产生上述解密金钥；以及

一加密 / 解密函式，根据上述解密金钥解密上述加密安全数据以获得上述安全数据。

5. 一种管理一安全可携式媒体的方法，其中上述安全可携式媒体包括一非易失性存储器以及一控制器，上述非易失性存储器是对应于一媒体识别码，且上述非易失性存储器分为一公开区、一隐藏区以及一保留隐藏区以储存数据，以及上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元，上述管理安全可携式媒体方法包括：

储存一第一固件和一第二固件于上述保留隐藏区中，分别用以撷取上述媒体识别码和由上述隐藏区存取数据；

由一外部装置传送一安全数据至上述安全可携式媒体；

由上述控制器使用上述第一固件由上述非易失性存储器撷取上述媒体识别码；

根据由上述第一固件提供的上述媒体识别码，通过储存于上述空开区的一安全程序产生一加密金钥；

根据上述加密金钥，通过上述安全程序加密上述安全数据以获得一加密安全数据；以及

由上述控制器使用上述第二固件将上述加密安全数据写入上述隐藏区中。

6. 根据权利要求 5 所述的管理上述安全可携式媒体的方法，还包括：

当由上述安全可携式媒体撷取上述安全数据时，通过上述控制器由上述隐藏区中读取上述加密安全数据；

通过上述控制器由上述非易失性存储器撷取上述媒体识别码；

根据上述第一固件提供的上述媒体识别码，通过上述安全程序产生一解密金钥；以及

根据上述解密金钥，通过上述安全程序解密上述加密安全数据以获得上述安全数据。

7. 一种安全可携式媒体包括：

一非易失性存储器，对应于一媒体识别码，且包括一公开区、一隐藏区、一保留隐藏区以存取数据，其中用以撷取上述媒体识别码的一第一固件，以及用以由隐藏区存取数据的一第二固件是储存于上述保留隐藏区中，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元；

一控制器，由一外部装置接收一执行程序；以及

一安全程序，储存于上述公开区，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码，产生相应上述执行程序和上述非易失性存储器的一第一程序识别码，以及使用上述第二固件将上述第一程序识别码写入上述隐藏区中，

其中上述执行程序和上述安全程序相连接。

8. 根据权利要求 7 所述的安全可携式媒体，其中上述安全程序使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码，产生相应上述执行程序和上述非易失性存储器一第二程序识别码，使用上述第二固件由上述隐藏区读取上述第一程序识别码，且比较上述第二程序识别码和上述第一程序识别码，当第二程序识别码和上述第一程序识别码相同时，持续执行上述执行程序，当第二程序识别码和上述第一程序识别码不同时，停止执行上述执行程序。

9. 根据权利要求 8 所述的安全可携式媒体，其中上述安全程序包括：

一固件链接库，启动上述第一固件由上述非易失性存储器撷取上述媒体识别码，启动上述第二固件将上述第一程序识别码写入上述隐藏区中，以及启动上述第二固件由上述隐藏区读取上述第一程序识别码；以及

一认证函式，根据上述第一固件提供的上述媒体识别码，产生相应上述执行程序和上述非易失性存储器上述第一程序识别码，根据上述媒体识别码，产生相应上述执行程序和上述非易失性存储器上述第二程序识别码，以及比较上述第二程序识别码和上述第一程序识别码。

10. 一种管理一安全可携式媒体的方法，其中上述安全可携式媒体包括一非易失性存储器以及一控制器，上述非易失性存储器是对应于一媒体识别码，且上述非易失性存储器分为一公开区、一隐藏区以及一保留隐藏区以存取数据，以及上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元，上述管理安全可携式媒体方法包括：

储存一第一固件和一第二固件于上述保留隐藏区中，分别用以撷取上述媒体识别码和由上述隐藏区存取数据；

由一外部装置传送一执行程序至上述安全可携式媒体；

由上述控制器使用上述第一固件由上述非易失性存储器撷取上述媒体识别码；

根据由上述第一固件提供的上述媒体识别码，通过一安全程序产生相应上述执行程序和上述非易失性存储器的一第一程序识别码；以及

由上述控制器使用上述第二固件将上述第一程序识别码写入上述隐藏区中。

11. 根据权利要求 10 所述的管理上述安全可携式媒体的方法，还包括

当执行上述执行程序时，通过上述控制器使用上述第一固件由上述非易失性存储器撷取媒体识别码；

根据由上述第一固件提供的上述媒体识别码，通过上述安全程序产生相应上述执行程序和上述非易失性存储器的一第二程序识别码；

由上述控制器使用上述第二固件由读取上述第一程序识别码，以及比较上述第二程序识别码和上述第一程序识别码；

当第二程序识别码和上述第一程序识别码相同时，持续执行上述执行程序；以及

当第二程序识别码和上述第一程序识别码不同时，停止执行上述执行程序。

12. 一种安全可携式媒体，连结至具有一数字权利管理代理的一客户端，包括：

一非易失性存储器，对应于一媒体识别码，且包括一公开区、一隐藏区、一保留隐藏区以存取数据，其中用以撷取上述媒体识别码的一第一固件，以及用以由隐藏区存取数据的一第二固件是储存于上述保留隐藏区中，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元；

一控制器，由上述客户端装置的上述数字权利管理代理接收一权利对象和一安全数据；以及

一安全可携式媒体代理，储存于上述公开区，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码，产生一加密金钥，根据上述加密金钥加密上述权利对象和上述安全数据以获得一加密权利对象和一加密安全数据，以及使用上述第二固件将上述加密权利对象和上述加密安全数据写入上述隐藏区中。

13. 根据权利要求 12 所述的安全可携式媒体，其中安全可携式媒体代理包括：

一固件链接库，启动上述第一固件由上述非易失性存储器撷取上述媒体识别码，以及启动上述第二固件将上述加密权利对象和上述加密安全数据写入上述隐藏区中；

一金钥产生函式，根据上述第一固件提供的上述媒体识别码产生上述加密金钥；以及

一加密 / 解密函式，根据上述加密金钥加密上述权利对象和上述安全数据以获得上述加密权利对象和上述加密安全数据。

14. 根据权利要求 12 所述的安全可携式媒体，其中当由上述安全可携式媒体撷取上述权利对象和上述安全数据时，上述安全可携式媒体代理由上述隐藏区读取上述权利对象和上述安全数据，且由上述非易失性存储器撷取上述媒体识别码，根据由上述第一固件提供的上述媒体识别码产生一解密金钥，以及根据上述解密金钥解密上述加密权利对象和上述加密安全数据以获得上述权利对象和上述安全数据。

15. 根据权利要求 14 所述的安全可携式媒体，其中上述安全可携式媒体代理包括：

一固件链接库，启动上述第二固件由隐藏区读取上述加密权利对象和上述加密安全数据，以及启动上述第一固件由上述非易失性存储器撷取上述媒体识别码；

一金钥产生函式，根据上述第一固件提供的上述媒体识别码产生上述解密金钥；以及

一加密 / 解密函式，根据上述解密金钥解密上述加密权利对象和上述加密安全数据以

获得上述权利对象和上述安全数据。

16. 根据权利要求 14 所述的安全可携式媒体，其中当上述加密权利对象和上述加密安全数据解密获得上述权利对象和上述安全数据时，上述安全可携式媒体传送上述权利对象和上述安全数据至上述客户端装置，上述数字权利管理代理使用上述权利对象以取得一数字权利管理内容，以及上述客户端装置的上述数字权利管理代理回传一权利对象信息至上述安全可携式媒体。

17. 根据权利要求 16 所述的安全可携式媒体，其中上述安全可携式媒体由上述客户端装置接收上述权利对象信息时，上述安全可携式媒体代理由上述隐藏区读取读取上述加密权利对象，由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码产生上述解密金钥，根据上述解密金钥，解密上述加密权利对象以获得上述权利对象，根据上述权利对象信息，修正上述权利对象以获得一修正权利对象，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件所提供的上述媒体识别码产生上述加密金钥，根据上述加密金钥加密上述修正权利对象以获得一加密修正权利对象，以及使用上述第二固件将上述加密修正权利数据写入上述隐藏区中。

18. 一种管理一安全可携式媒体的方法，其中上述安全可携式媒体连结至具有一数字权利管理代理的一客户端，上述安全可携式媒体包括一非易失性存储器和一控制器，上述非易失性存储器对应于一媒体识别码，且分为一公开区、一隐藏区、一保留隐藏区以存取数据，其中用以撷取上述媒体识别码的一第一固件，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元，包括：

储存一安全可携式媒体代理在上述非易失性存储器的上述公开区中；

储存一第一固件和一第二固件在上述保留隐藏区中，用以分别撷取上述媒体识别码和于上述隐藏区存取数据；

由上述客户端装置的上述数字权利管理代理传送一权利对象和一安全数据；

执行上述安全可携式媒体代理以使用上述第一固件由上述非易失性存储器撷取上述媒体识别码；

根据由上述第一固件提供的上述媒体识别码，执行上述安全可携式媒体代理以产生一加密金钥；

根据上述加密金钥，执行上述安全可携式媒体代理加密上述权利对象和上述安全数据以获得一加密权利对象和一加密安全数据；

执行上述安全可携式媒体代理以使用上述第二固件将上述加密权利对象和上述加密安全数据写入上述隐藏区中。

19. 根据权利要求 18 所述的管理上述安全可携式媒体的方法，还包括：

当由上述安全可携式媒体撷取上述权利对象和上述安全数据时，执行上述安全可携式媒体代理由上述隐藏区读取上述加密权利对象和上述加密安全数据；

执行上述安全可携式媒体代理由上述非易失性存储器撷取上述媒体识别码；

根据上述第一固件提供的上述媒体识别码，执行上述安全可携式媒体代理产生一解密金钥；以及

根据上述解密金钥，执行上述安全可携式媒体代理将上述加密权利对象和上述加密安全数据解密以获得上述权利对象和上述安全数据。

20. 根据权利要求 19 所述的管理上述安全可携式媒体的方法还包括 :

当上述加密权利对象和上述加密安全数据解密而获得上述权利对象和上述安全数据后,由上述安全可携式媒体传送上述权利对象和上述安全数据至上述客户端装置 ;

通过上述数字权利管理代理使用上述权利对象以取得一数字权利管理代理内容 ;以及

通过上述数字权利管理代理回传一权利对象信息至上述安全可携式媒体。

21. 根据权利要求 20 所述的管理上述安全可携式媒体的方法,还包括 :

在上述安全可携式媒体由上述客户端装置接收上述权利对象后,执行上述安全可携式媒体代理由上述隐藏区读取上述加密权利对象 ;

由上述非易失性存储器执行上述安全可携式媒体代理以撷取上述媒体识别码 ;

根据上述第一固件提供的上述媒体识别码,执行上述安全可携式媒体代理产生上述解密金钥 ;

根据上述解密金钥,执行上述安全可携式媒体代理解密上述加密权利对象 ;

根据上述权利对象信息,执行上述安全可携式媒体代理修改上述权利对象以产生一修改权利对象 ;

执行上述安全可携式媒体代理以使用上述第一固件由上述非易失性存储器撷取上述媒体识别码 ;

根据上述第一固件提供的上述媒体识别码,执行上述安全可携式媒体代理产生上述加密金钥 ;

根据上述加密金钥,执行上述安全可携式媒体代理加密上述修改权利对象以获得一加密修改权利对象 ;以及

执行上述安全可携式媒体代理以使用上述第二固件将上述加密修改权利对象写入上述隐藏区中。

22. 根据权利要求 18 所述的管理上述安全可携式媒体的方法,上述安全可携式媒体为一安全数码存储卡、一多媒体存储卡或一通用序列总线随身盘。

安全可携式媒体以及管理安全可携式媒体的方法

技术领域

[0001] 本发明主要是有关于数据存取，特别是有关于安全数据的存取。

背景技术

[0002] 数字权利管理 (Digital Rights Management，DRM) 是一种应用在存取控制中保护数字数据的技术，硬件制造商、出版商、权利所有人都使用此技术来保护数字数据的内容。数字权利管理技术通过防止来自使用者的未授权的存取、复制以及转档的操作来保护控制数字媒体的使用。数字权利管理技术已使用在许多公司的产品中，像是 SONY、Amazon、Apple、Microsoft 等。

[0003] 当一使用者端想要播放一数字内容，使用者端就由一数字权利管理服务器下载数字内容至客户端 (client-end) 装置，且数字权利管理服务器发布一权利对象至客户端装置。使用者端就能根据权利对象播放储存在客户端装置的数字内容。若数字内容由授权的装置复制至未授权的装置，因为未授权装置无法存取一权利对象，因此使用者端将无法播放复制至未授权装置的数字内容。因为一般数字权利管理服务器不允许使用者端移动一权利对象由客户端装置至其它装置中，因此，使用者端只能播放已连结至数字权利管理服务器并经由网络连结来获得相关权利对象的客户端装置的数字内容。这对使用者而言是相当不方便的。

[0004] 开放移动通讯联盟 (Open Mobile Alliance，OMA) 已建立一开放移动通讯联盟数字权利管理 2.0/2.1(OMA DRM2.0/2.1) 标准，在此标准中，允许使用者从一客户端装置移动一权利对象至一安全可携式媒体 (Secure Removable Media，SRM) 中。举例来说，安全可携式媒体可为一安全数码存储卡 (Secure Digital card，SD card)、一通用序列总线 (Universal Serial Bus，USB) 随身盘或一多媒体存储卡 (Multi-Media Card，MMC)。因此，使用者端可使用存取在可携式媒体的权利对象，来播放存取在可携式媒体的数字内容，这样的做法可视为使用者端的使用。然而，安全可携式媒体 (SRM) 标准并未提到在安全可携式媒体中如何以安全的方式储存和撷取权利对象。因此，需要一种根据 OMA DRM2.0/2.1 标准来管理储存在安全可携式媒体的权利对象的方法。

发明内容

[0005] 本发明一实施例提供一种安全可携式媒体包括：一非易失性存储器，对应于一媒体识别码，且包括一公开区、一隐藏区、一保留隐藏区以存取数据，其中用以撷取上述媒体识别码的一第一固件，以及用以由隐藏区存取数据的一第二固件是储存于上述保留隐藏区中，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元；一控制器，由一外部装置接收一安全数据；以及一安全程序，储存于上述公开区，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码产生一加密金钥，通过上述加密金钥加密上述安全数据以获得一加密安全数据，以及使用上述第二固件将上述加密安全数据写入上述隐藏区中。

[0006] 本发明一实施例提供一种管理一安全可携式媒体的方法，其中上述安全可携式媒体包括一非易失性存储器以及一控制器，上述非易失性存储器对应于一媒体识别码，且上述非易失性存储器可分为一公开区、一隐藏区以及一保留隐藏区以存取数据，以及上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元，上述管理安全可携式媒体方法包括：储存一第一固件和一第二固件于上述保留隐藏区中，分别用以撷取上述媒体识别码和由上述隐藏区存取数据；由一外部装置传送一安全数据至上述安全可携式媒体；由上述控制器使用上述第一固件由上述非易失性存储器撷取上述媒体识别码；根据由上述第一固件提供的上述媒体识别码，通过储存于上述空开区的一安全程序产生一加密金钥；根据上述加密金钥，通过上述安全程序加密上述安全数据以获得一加密安全数据；以及由上述控制器使用上述第二固件将上述加密安全数据写入上述隐藏区中。

[0007] 本发明一实施例提供一种安全可携式媒体包括：一非易失性存储器，对应于一媒体识别码，且包括一公开区、一隐藏区、一保留隐藏区以存取数据，其中用以撷取上述媒体识别码的一第一固件，以及用以由隐藏区存取数据的一第二固件是储存于上述保留隐藏区中，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元；一控制器，由一外部装置接收一执行程序；以及一安全程序，储存于上述公开区，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码，产生相应上述执行程序和上述非易失性存储器的一第一程序识别码，以及使用上述第二固件将上述第一程序识别码写入上述隐藏区中，其中上述执行程序和上述安全程序相连结。

[0008] 本发明一实施例提供一种管理一安全可携式媒体的方法，其中上述安全可携式媒体包括一非易失性存储器以及一控制器，上述非易失性存储器对应于一媒体识别码，且上述非易失性存储器可分为一公开区、一隐藏区以及一保留隐藏区以存取数据，以及上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元，上述管理安全可携式媒体方法包括：储存一第一固件和一第二固件于上述保留隐藏区中，分别用以撷取上述媒体识别码和由上述隐藏区存取数据；由一外部装置传送一执行程序至上述安全可携式媒体；由上述控制器使用上述第一固件由上述非易失性存储器撷取上述媒体识别码；根据由上述第一固件提供的上述媒体识别码，通过一安全程序产生相应上述执行程序和上述非易失性存储器的一第一程序识别码；以及由上述控制器使用上述第二固件将上述第一程序识别码写入上述隐藏区中。

[0009] 本发明一实施例提供一种安全可携式媒体，连结至具有一数字权利管理 (DRM) 代理的一客户端，包括：一非易失性存储器，对应于一媒体识别码，且包括一公开区、一隐藏区、一保留隐藏区以存取数据，其中用以撷取上述媒体识别码的一第一固件，以及用以由隐藏区存取数据的一第二固件是储存于上述保留隐藏区中，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元；一控制器，由上述客户端装置的上述 DRM 代理接收一权利对象和一安全数据；以及一安全可携式媒体 (SRM) 代理，储存于上述公开区，使用上述第一固件由上述非易失性存储器撷取上述媒体识别码，根据上述第一固件提供的上述媒体识别码，产生一加密金钥，根据上述加密金钥加密上述权利对象和上述安全数据以获得一加密权利对象和一加密安全数据，以及使用上述第

二固件将上述加密权利对象和上述加密安全数据写入上述隐藏区中。

[0010] 本发明一实施例提供一种管理一安全可携式媒体的方法，其中上述安全可携式媒体连结至具有一数字权利管理 (DRM) 代理的一客户端，上述安全可携式媒体包括一非易失性存储器和一控制器，上述非易失性存储器对应于一媒体识别码，且分为一公开区、一隐藏区、一保留隐藏区以储存数据，其中用以撷取上述媒体识别码的一第一固件，且上述媒体识别码被物理铭刻在上述非易失性存储器的一半导体芯片上，且不会储存于一正规存储器单元，包括：储存一 SRM 代理在上述非易失性存储器的上述公开区中；储存一第一固件和一第二固件在上述保留隐藏区中，用以分别撷取上述媒体识别码和于上述隐藏区存取数据；由上述客户端装置的上述 DRM 代理传送一权利对象和一安全数据；执行上述 SRM 代理以使用上述第一固件由上述非易失性存储器撷取上述媒体识别码；根据由上述第一固件提供的上述媒体识别码，执行上述 SRM 代理以产生一加密金钥；

[0011] 根据上述加密金钥，执行上述 SRM 代理加密上述权利对象和上述安全数据以获得一加密权利对象和一加密安全数据；执行上述 SRM 代理以使用上述第二固件将上述加密权利对象和上述加密安全数据写入上述隐藏区中。

附图说明

[0012] 图 1 是显示根据本发明的实施例所述的安全可携式媒体 100 的方块图。

[0013] 图 2 是显示根据本发明的实施例所述的安全程序 200 的方块图。

[0014] 图 3A 是显示根据本发明一实施例所述的流程图 300。

[0015] 图 3B 是显示根据本发明一实施例所述的流程图 350。

[0016] 图 4A 是显示根据本发明一实施例所述的流程图 400。

[0017] 图 4B 是显示根据本发明一实施例所述的流程图 450。

[0018] 图 5 是显示根据本发明一实施例所述的数字权利管理 (DRM) 系统 500 的方块图。

[0019] 图 6 是显示根据本发明一实施例所述的 DRM 系统 500 的安全可携式媒体 600 的方块图。

[0020] 图 7 是显示根据本发明一实施例所述的安全可携式媒体代理 700 的方块图。

[0021] 图 8A 是显示根据本发明一实施例所述的流程图 800。

[0022] 图 8B 是显示根据本发明一实施例所述的流程图 850。

[0023] 图 9A 和图 9B 是显示根据本发明一实施例所述的 DRM 内容的局部使用的流程图 900。

[0024] [主要元件标号说明]

[0025] 100、506 ～安全可携式媒体；102、602 ～控制器；

[0026] 104 ～非易失性存储器；110、610 ～公开区；

[0027] 112、200 ～安全程序；114、202、614、702 ～固件链接库；

[0028] 116 ～执行程序；120、620 ～隐藏区；

[0029] 122、629 ～安全数据；124 ～程序识别码；

[0030] 130、630 ～保留隐藏区；132、134、632、634 ～固件；

[0031] 140、640 ～逻辑和物理地址对照表；204、704 ～金钥产生函式；

[0032] 206、706 ～加密 / 解密函式；208、708 ～认证函式；

[0033] 300、350、400、450、800、850、900 ～流程图；

[0034] 500 ～数字权利管理系统； 502 ～ DRM 服务器；

[0035] 508 ～权利发行； 510 ～封包；

[0036] 512、512'、618 ～ DRM 代理； 514、514'、616 ～内容浏览器；

[0037] 516、516' ～权利对象 / 安全数据； 622 ～权利对象；

[0038] 518、518'、619 ～ DRM 内容；

[0039] 522、612、700 ～安全可携式媒体代理；

[0040] 710 ～ DRM 要求函式。

具体实施方式

[0041] 本章节所叙述的是实施本发明的最佳方式，目的在于说明本发明的精神而非用以限定本发明的保护范围，本发明的保护范围当视所附的申请专利范围所界定者为准。

[0042] 图 1 是显示根据本发明的实施例所述的安全可携式媒体 100 的方块图，其中安全可携式媒体 100 可用以储存安全数据。在一实施例中，安全可携式媒体 100 包括一控制器 102 以及一非易失性存储器 104。安全可携式媒体 100 可为一安全数码存储卡 (Secure Digital card，SD card)、一多媒体存储卡 (Multi-Media Card，MMC) 或一通用序列总线 (Universal Serial Bus，USB) 随身盘。非易失性存储器 104 具有一媒体识别码的唯一识别码 (Unique Identity，UID)，且因此可根据由固件 132 产生的媒体识别码 UID 来识别安全可携式媒体 100。媒体识别码 UID 是物理铭刻在非易失性存储器 104 的半导体芯片上，且不会储存于正规非易失性存储器单元或单次可程序 (one-time-programmabel) 存储器，例如只读存储器 (read only memory，ROM) 中。在一实施例中，媒体识别码 UID 是一芯片序号，标示在非易失性存储器 104 的芯片上。因为媒体识别码 UID 不会储存于非易失性存储器 104 的正规非易失性存储器单元上，媒体识别码 UID 不能经由一位对位 (bit-to-bit) 镜射的方式来复制。

[0043] 在一实施例中，非易失性存储器 104 的储存空间分为一公开区 (public area)110、一隐藏区 (hidden area)120 以及一保留隐藏区 (reserved hidden area)130。储存空间的公开区 110 可被随选的使用者端存取。储存空间的隐藏区 120 以及保留隐藏区 130 则不可被使用者端存取。一逻辑和物理地址对照表 140 储存在非易失性存储器 104 中。固件 132 和固件 134 储存在非易失性存储器 104 的保留隐藏区 130 中。固件 132 用以由非易失性存储器 104 读取媒体识别码 UID。在一实施例中，固件 132 包括一对一镜射算法。在固件 132 由非易失性存储器 104 读取媒体识别码 UID 后，固件 132 使用一对一镜射算法由原来的媒体识别码 UID 推导出一新的媒体识别码 UID。因此，固件 132 输出的媒体识别码 UID 将不同于原为了安全目的物理铭刻在非易失性存储器 104 的半导体芯片上的媒体识别码 UID。一对一镜射算法可以提供额外的保护。因此，即使存储器单元制造商缺少原来的媒体识别码 UID，未经授权的装置仍然无法得知使用原来的媒体识别码 UID 所产生的一加密金钥和一解密金钥。固件 134 用以读取来自隐藏区 120 的数据，或写入数据至隐藏区 120。一安全程序 112 以及一固件链接库 114 储存在在非易失性存储器 104 的公开区 110 中。

[0044] 安全程序 112 用以储存安全数据至非易失性存储器 104 的隐藏区 120 中，且由隐藏区 120 中撷取安全数据。安全程序 112 更进一步的功能将在图 2、图 3A 和图 3B 中详述。

固件链接库 114 用以启动且呼叫固件 132 和固件 134。在一实施例中，固件链接库 114 为安全程序 112 的一部分。

[0045] 图 2 是显示根据本发明的实施例所述的安全程序 200 的方块图。当安全可携式媒体 100 由一外部装置接收安全数据时，安全程序 200 将安全数据储存至非易失性存储器 104 的隐藏区 120 中。在一实施例中，安全程序 200 包括一固件链接库 202，一金钥产生函式 204、一加密 / 解密函式 206 以及一认证函式 208。固件链接库 202 用以启动固件 132 和固件 134 来读取媒体识别码 UID 或存取于隐藏区 120。在固件 132 产生媒体识别码 UID 后，金钥产生函式 204 根据固件 132 所产生的媒体识别码 UID 产生一加密金钥或一解密金钥。因为金钥产生函式 204 是一对一函式，因此不同加密金钥对应至不同安全可携式媒体的非易失性存储器，以及不同解密金钥对应至不同安全可携式媒体的非易失性存储器。加密 / 解密函式 206 用以根据一加密金钥加密安全数据或根据一解密金钥解密已加密的安全数据。认证函式 208 用以定义是否在已认证的安全可携式媒体 100 中执行一执行程序 116。

[0046] 图 3A 是显示根据本发明一实施例所述的流程图 300，其适用于写入安全数据至一安全可携式媒体 100 中。当安全可携式媒体 100 从一外部装置接收需要安全储存的安全数据时（步骤 302），安全程序 112 为了撷取来自非易失性存储器 104 的媒体识别码 UID，使用固件链接库 114 以启动固件 132（步骤 304）。接着，安全程序 112 根据固件 132 产生的媒体识别码 UID 使用金钥产生函式 204 产生加密金钥（步骤 306）。安全程序 112 根据加密金钥使用加密 / 解密函式 206 加密安全数据以得到一加密安全数据 122（步骤 308）。为了将加密安全数据 122 写入至隐藏区 120 中，数据安全程序 112 使用固件链接库 114 以启动固件 134（步骤 310）。因为加密安全数据 122 储存在隐藏区 120 中，使用者端无法直接存取加密安全数据 122。即使加密安全数据 122 已成功复制至未认证的装置中，但因为未认证的装置中未包括原非易失性存储器 104 的媒体识别码 UID，未认证的装置无法产生正确的解码金钥来解码加密安全数据 122。

[0047] 图 3B 是显示根据本发明一实施例所述的流程图 350，其适用于读取安全数据至一安全可携式媒体 100 中。首先，当安全数据被读取时，为了读取来自非易失性存储器 104 的隐藏区 120 的加密安全数据 122，安全程序 112 使用固件链接库 114 以呼叫固件 134（步骤 352）。接着，为了撷取非易失性存储器 104 的媒体识别码 UID，安全程序 112 使用固件链接库 114 以呼叫固件 132（步骤 354）。安全程序 112 根据固件 132 产生的媒体识别码 UID 使用金钥产生函式 204 产生一解密金钥（步骤 356）。安全程序 112 根据解密金钥使用加密 / 解密函式 206 来解密加密安全数据 122 以得到安全数据（步骤 358）。安全程序 112 根据通讯协议使用安全数据或传送安全数据至外部的装置（步骤 360）。

[0048] 一执行程序也需要储存于安全防护中。然而，执行程序不能以加密的形式来储存。处理器不能直接执行加密后的执行程序。为了预防执行程序在未认证的装置执行，在执行执行程序之前，安全程序必须判定储存执行程序的装置是否为一未认证装置。图 4A 是显示根据本发明一实施例所述的流程图 400，其适用于写入执行程序 116 至安全可携式媒体 100 中。首先，写入执行程序 116 至非易失性存储器 104 的公开区 110 中。执行程序 116 是动态或静态连结至安全程序 112（步骤 402）。为了撷取来自非易失性存储器 104 的媒体识别码 UID，安全程序 112 使用固件链接库 114 呼叫固件 132（步骤 404）。安全程序 112 根据固件 132 产生的媒体识别码 UID，使用认证函式 208 产生一程序识别码 UID’ 124（步骤 406），

其中程序识别码 UID’ 124 是对应执行程序 116 和非易失性存储器 104。换句话说，不同安全可携式媒体的不同执行程序或不同非易失性存储器对应不同程序识别码。最后，为了写入程序识别码 UID’ 124 至非易失性存储器 104 的隐藏区 120，安全程序 112 使用固件链接库 114 呼叫固件 134（步骤 408）。

[0049] 图 4B 是显示根据本发明一实施例所述的流程图 450，其适用于写入执行程序 116 至安全可携式媒体 100 中。首先，为了撷取来自非易失性存储器 104 的媒体识别码 UID，执行程序 116 使用固件链接库 114 呼叫固件 132（步骤 452）。执行程序 116 使用安全程序 112 的认证函式 208 以比较由固件 132 产生的媒体识别码 UID 和程序识别码 UID’ 124（步骤 454、456）。在一实施例中，执行程序 116 根据固件 132 产生的媒体识别码 UID，使用认证函式 208 产生一第二程序识别码 UID”，执行程序 116 使用固件链接库 114 呼叫固件 134 以读取来自隐藏区 120 的程序识别码 UID’ 124 以及，执行程序 116 根据固件 132 产生的媒体识别码 UID，使用认证函式 208 以比较储存于隐藏区 120 的程序识别码 UID’ 124 和第二程序识别码 UID”。

[0050] 认证函式 208 决定第二程序识别码 UID”是否和程序识别码 UID’ 124 相同。若安全可携式媒体 100 为一具有执行程序 116 的已认证安全可携式媒体，根据非易失性存储器 104 的媒体识别码 UID 产生的第二程序识别码 UID”必须和储存于隐藏区 120 的程序识别码 UID’124 相同，才可使得执行程序 116 可以持续的执行（步骤 458），其中执行程序 116 原先已储存于安全可携式媒体 100 中。若安全可携式媒体 100 不为一具有执行程序 116 的已认证安全可携式媒体，根据非认证的安全可携式媒体 100 的固件 132 提供的媒体识别码 UID 产生的第二程序识别码 UID”必须和储存于隐藏区 120 的程序识别码 UID’ 124 不同，才可使得执行程序 116 终止（步骤 460），其中执行程序 116 原先已储存于安全可携式媒体 100 中。也就是说，即使将执行程序 116 复制至一非认证装置的非易失性存储器，执行程序 116 仍不能执行于非认证装置中。

[0051] 图 5 是显示根据本发明一实施例所述的数字权利管理 (DRM) 系统 500 的方块图。在一实施例中，数字权利管理 (DRM) 系统 500 包括一 DRM 服务器 502、一客户端装置 504 以及一安全可携式媒体 506。DRM 服务器 502 包括一权利发行 508 以及一封包 510。客户端装置 504 经由网络连结至 DRM 服务器 502。举例来说，客户端装置 504 可为一个人计算机或移动电话。在一实施例中，客户端装置 504 包括一 DRM 代理 512 以及一内容浏览器 514。当客户端装置 504 想要播放或使用一 DRM 内容，客户端装置 504 的 DRM 代理 512 传送一请求至 DRM 服务器 502，且 DRM 服务器 502 的权利发行 508 传送一权利对象 / 安全数据 516 至客户端装置 504，其中 DRM 服务器 502 的封包 510 传送 DRM 内容 518 至客户端装置 504。在一实施例中，安全数据为一公开金钥、一秘密金钥或一凭证。客户端装置 504 的内容浏览器 514 可根据权利对象 / 安全数据 516 播放或使用 DRM 内容 518。

[0052] 安全可携式媒体 506 连结至客户端装置 504。举例来说，安全可携式媒体 506 可为一 SD 卡、MMC 卡或一 USB 随身盘。在一实施例中，安全可携式媒体 506 经由 USB 接头连结至客户端装置 504，且包含一安全可携式媒体代理 522。客户端装置 504 可将 DRM 内容 518 写入安全可携式媒体 506 中，如 DRM 内容 518’ 所示。客户端装置 504 可移动客户端装置 504 和安全可携式媒体 506 之间的权利对象 / 安全数据 516。在一实施例中，安全可携式媒体 506 也包括 DRM 代理 512 和内容浏览器 514。当权利对象 / 安全数据 516 移动至安全可携

式媒体 506，安全可携式媒体 506 可直接根据权利对象 / 安全数据 516 播放或使用 DRM 内容 518。

[0053] 当权利对象 / 安全数据 516 由客户端装置 504 移动至安全可携式媒体 506 时，安全可携式媒体代理 522 将权利对象 / 安全数据 516 加密以获得加密的权利对象 / 安全数据 516，且安全可携式媒体代理 522 将加密的权利对象 / 安全数据 516' 写入安全可携式媒体 506 的隐藏区。因为储存于安全可携式媒体 506 的加密的权利对象 / 安全数据 516' 储存于隐藏区中，使用者无法由安全可携式媒体 506 直接复制加密的权利对象 / 安全数据 516'。此外，因为储存于安全可携式媒体 506 的加密的权利对象 / 安全数据 516' 已被加密，使用者无法直接使用由安全可携式媒体 506 所复制的加密的权利对象 / 安全数据 516'。因此，DRM 系统 500 的权利对象可免于未经授权的存取或复制。

[0054] 图 6 是显示根据本发明一实施例所述的 DRM 系统 500 的安全可携式媒体 600 的方块图。在一实施例中，安全可携式媒体 600 包括一控制器 602 以及一非易失性存储器 604。安全可携式媒体 600 可为一 SD 卡、MMC 卡或一 USB 随身盘。非易失性存储器 604 具有一对应的媒体识别码 UID，因此，可根据媒体识别码 UID 来识别安全可携式媒体 600。媒体识别码 UID 为一刻入非易失性存储器 604 的半导体芯片上的序号，且不会储存于正规非易失性存储器单元或单次可程序存储器，像是只读存储器 (read only memory，ROM) 中。在一实施例中，媒体识别码 UID 是一芯片序号，标示在非易失性存储器 604 的芯片上。因为媒体识别码 UID 不会储存于非易失性存储器 604 的正规非易失性存储器单元上，媒体识别码 UID 不能经由一位对位 (bit-to-bit) 镜射的方式来复制。

[0055] 在一实施例中，非易失性存储器 604 的储存空间分为一公开区 610、一隐藏区 620 以及一保留隐藏区 630。储存空间的公开区 610 可被随选的使用者端存取。在一实施例中，一安全可携式媒体代理 612、固件链接库 614、一内容浏览器 616、一 DRM 代理 618 以及一 DRM 内容储存于公开区 610 中。储存空间的隐藏区 620 以及保留隐藏区 630 则不可被使用者端存取。一逻辑和物理地址对照表 640 储存在非易失性存储器 604 中。固件 632 和固件 634 储存在非易失性存储器 604 的保留隐藏区 630 中。固件 632 用以由非易失性存储器 604 读取媒体识别码 UID。在一实施例中，固件 632 包括一对一镜射算法。在固件 632 由非易失性存储器 604 读取媒体识别码 UID 后，为了安全的目的，固件 632 使用一对一镜射算法由原来的媒体识别码 UID 推导出一新的媒体识别码 UID。固件 634 用以读取来自隐藏区 620 的数据，或写入数据至隐藏区 620。在权利对象 622 和安全数据 629 储存于非易失性存储器 604 的隐藏区 620 之前，安全可携式媒体代理 612 用以加密权利对象 622 和安全数据 629。安全可携式媒体代理 612 更进一步的功能将在图 7、图 8A、图 8B 和图 9 中详述。固件链接库 614 用以启动且呼叫固件 632 和固件 634。在一实施例中，固件链接库 614 为安全可携式媒体代理 612 的一部分。

[0056] 图 7 是显示根据本发明一实施例所述的安全可携式媒体代理 700 的方块图。当安全可携式媒体 600 由一客户端接收一权利对象 622 和安全数据 629，安全可携式媒体代理 700 将权利对象 622 和安全数据 629 储存至非易失性存储器 604 的隐藏区 620。在一实施例中，安全可携式媒体代理 700 包括一固件链接库 702、一金钥产生函式 704、一加密 / 解密函式 706、一认证函式 708 以及一 DRM 要求函式 710。固件链接库 702 用以启动固件 632 和固件 634 来读取媒体识别码 UID 或存取于隐藏区 620。在固件 632 产生媒体识别码 UID 后，

金钥产生函式 704 根据固件 632 所产生的媒体识别码 UID 产生一加密金钥或一解密金钥。因为金钥产生函式 704 是一一对一函式，因此不同加密金钥对应至不同安全可携式媒体的非易失性存储器，以及不同解密金钥对应至不同安全可携式媒体的非易失性存储器。加密 / 解密函式 706 用以根据一加密金钥加密权利对象 622 和安全数据 629 或根据一解密金钥解密已加密的安全数据。

[0057] 图 8A 是显示根据本发明一实施例所述的流程图 800，其适用于写入权利对象 622 和安全数据 629 至一安全可携式媒体 600 中。首先，一客户端装置的 DRM 代理传送一权利对象 622 和一安全数据 629 至一安全可携式媒体代理 612（步骤 802），且安全可携式媒体代理 612 接收一第一加密权利对象、一第一加密安全数据以及一区段加密金钥（步骤 804）。接着，安全可携式媒体代理 612 使用区段解密金钥来解密第一加密权利对象和第一加密安全数据以获得权利对象 622 和安全数据 629（步骤 806）。接着，为了由非易失性存储器 604 撷取媒体识别码 UID，安全可携式媒体代理 612 使用固件链接库 614 以启动固件 632（步骤 808）。接着，根据固件 632 提供的媒体识别码 UID，安全可携式媒体代理 612 使用金钥产生函式 704 产生一加密金钥（步骤 810）。根据加密金钥，安全可携式媒体代理 612 使用加密 / 解密函式 706 加密权利对象 622 和安全数据 629 以获得一第二加密权利对象、一第二加密安全数据（步骤 812）。安全可携式媒体代理 612 使用固件链接库启动固件 634 以将第二加密权利对象和第二加密安全数据写入隐藏区 620（步骤 814）。因为第二加密权利对象和第二加密安全数据系储存于隐藏区 620 中，使用者端不能直接存取第二加密权利对象 622 和第二加密安全数据 629。即使第二加密权利对象 622 和第二加密安全数据 629 已成功复制至一未授权装置，但因为未授权装置未包括原非易失性存储器 604 的媒体识别码 UID，未授权装置并不能产生一正确的解密金钥来解密第二加密权利对象 622 和第二加密安全数据 629。

[0058] 图 8B 是显示根据本发明一实施例所述的流程图 850，其适用于由一安全可携式媒体 600 读取权利对象和安全数据。安全可携式媒体代理 612 使用固件链接库 614 呼叫固件 634 以由非易失性存储器 604 的隐藏区 620 读取第一加密权利对象和第一加密安全数据（步骤 852）。安全可携式媒体代理 612 使用固件链接库 614 呼叫固件 632 以由非易失性存储器 604 撷取媒体识别码 UID（步骤 854）。根据固件 632 提供的媒体识别码 UID，安全可携式媒体代理 612 使用金钥产生函式 704 产生一解密金钥（步骤 856）。根据一解密金钥，安全可携式媒体代理 612 使用加密 / 解密函式 706 解密第一加密权利对象和第一加密安全数据以获得权利对象 622 和安全数据 629（步骤 858）。根据权利对象 622 和安全数据 629，安全可携式媒体代理 612 加密一第二权利对象和一第二安全数据，且传送第二权利对象、第二安全数据以及一区段解密金钥至客户端装置的 DRM 服务器（步骤 860）。最后，DRM 服务器接收了第二权利对象、第二安全数据以及区段解密金钥（步骤 862）。

[0059] 图 9 是显示根据本发明一实施例所述的 DRM 内容的局部使用的流程图 900。首先，安全可携式媒体代理 612 使用固件链接库 614 由一隐藏区 620 读取第一加密权利对象 622 以及第一加密安全数据 629（步骤 901）。安全可携式媒体代理 612 使用固件链接库 614 撷取一对应安全可携式媒体 600 的媒体识别码 UID（步骤 902）。安全可携式媒体代理 612 使用金钥产生函式 704 以及固件 132 提供的媒体识别码 UID 产生一解密金钥（步骤 903）。安全可携式媒体代理 612 使用解密金钥以及加密 / 解密函式 706 将第一加密权利对象以及第

一加密安全数据解密以获得一权利对象 622 和安全数据 629(步骤 904)。安全可携式媒体代理 612 传送权利对象 622、安全数据 629 以及一区段解密金钥至客户端装置 504 的 DRM 代理 512(步骤 905)。DRM 代理 512 接收第二加密权利对象、第二加密安全数据以及区段解密金钥(步骤 906)。DRM 代理 512 使用区段解密金钥将第二加密权利对象和第二加密安全数据解密以获得权利对象 622 和安全数据 629,且使用获得的权利对象 622 和安全数据 629 来取得 DRM 内容(步骤 907)。DRM 代理 512 传送加密权利对象信息和区段解密金钥至安全可携式媒体代理 612(步骤 908)。安全可携式媒体代理 612 使用区段解密金钥将加密权利对象信息解密以获得权利对象信息(步骤 909)。

[0060] 安全可携式媒体代理 612 使用固件链接库 614 由隐藏区 620 读取第一加密权利对象和第一安全数据(步骤 910)。安全可携式媒体代理 612 使用固件链接库 614 撷取对应于安全可携式媒体 600 的媒体识别码 UID(步骤 911)。安全可携式媒体代理 612 使用金钥产生函式 704 以及固件 632 提供的媒体识别码 UID 产生一解密金钥(步骤 912)。安全可携式媒体代理 612 使用解密金钥以及加密 / 解密函式 706 将第一加密权利对象以及第一加密安全数据解密以获得一权利对象 622 和安全数据 629(步骤 913)。安全可携式媒体代理 612 使用权利对象信息来修正权利对象以产生一修正的权利对象(步骤 914)。安全可携式媒体代理 612 使用固件链接库 614 撷取固件 632 提供的媒体识别码 UID(步骤 915)。安全可携式媒体代理 612 使用金钥产生函式 704 以及固件 632 提供的媒体识别码 UID 产生一加密金钥(步骤 916)。根据修正的权利对象和安全数据,安全可携式媒体代理 612 使用加密金钥以及加密 / 解密函式 706 将第三加密权利对象以及第三加密安全数据加密(步骤 917)。安全可携式媒体代理 612 使用固件链接库 614 将第三加密权利对象以及第三加密安全数据写入隐藏区 620 中(步骤 918)。

[0061] 本章节所叙述的是实施本发明的最佳方式,目的在于说明本发明的精神而非用以限定本发明的保护范围,任何本领域技术人员,在不脱离本发明的精神和范围内,当可作些许的更动与润饰,因此本发明的保护范围当视所附的权利要求范围所界定者为准。

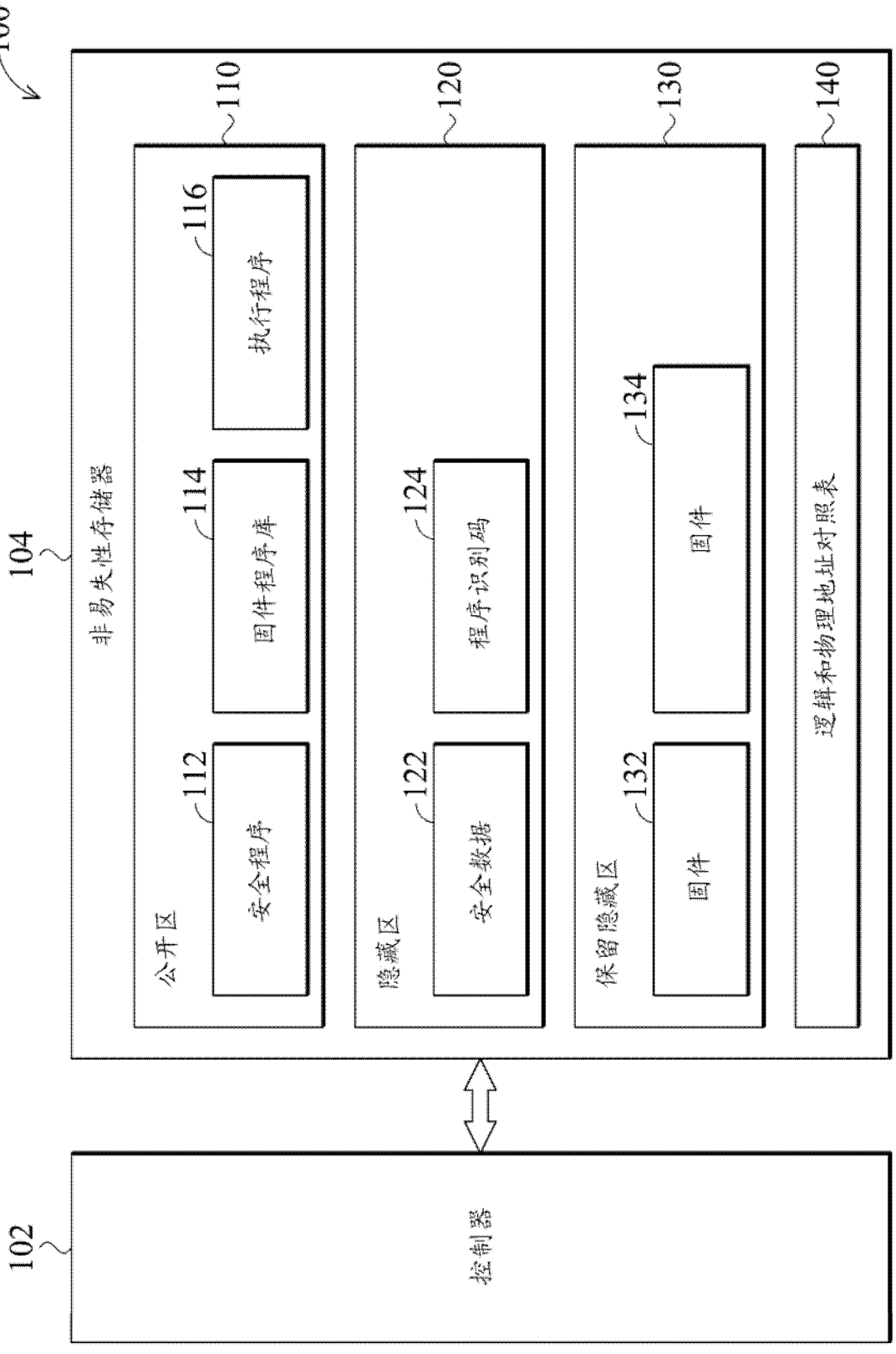

100
104
非易失性存储器
公开区
112
安全程序
114
固件程序库
116
执行程序
隐藏区
122
安全数据
124
程序识别码
保留隐藏区
132
固件
134
固件
逻辑和物理地址对照表
110
120
130
140
102
控制器

图 1

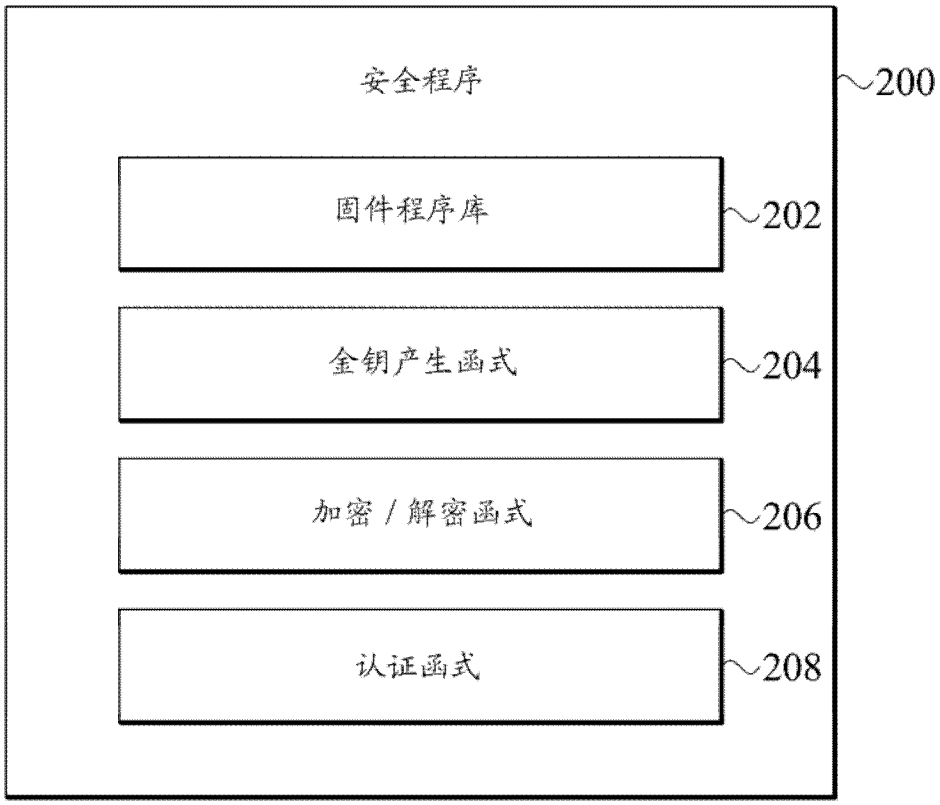


图 2

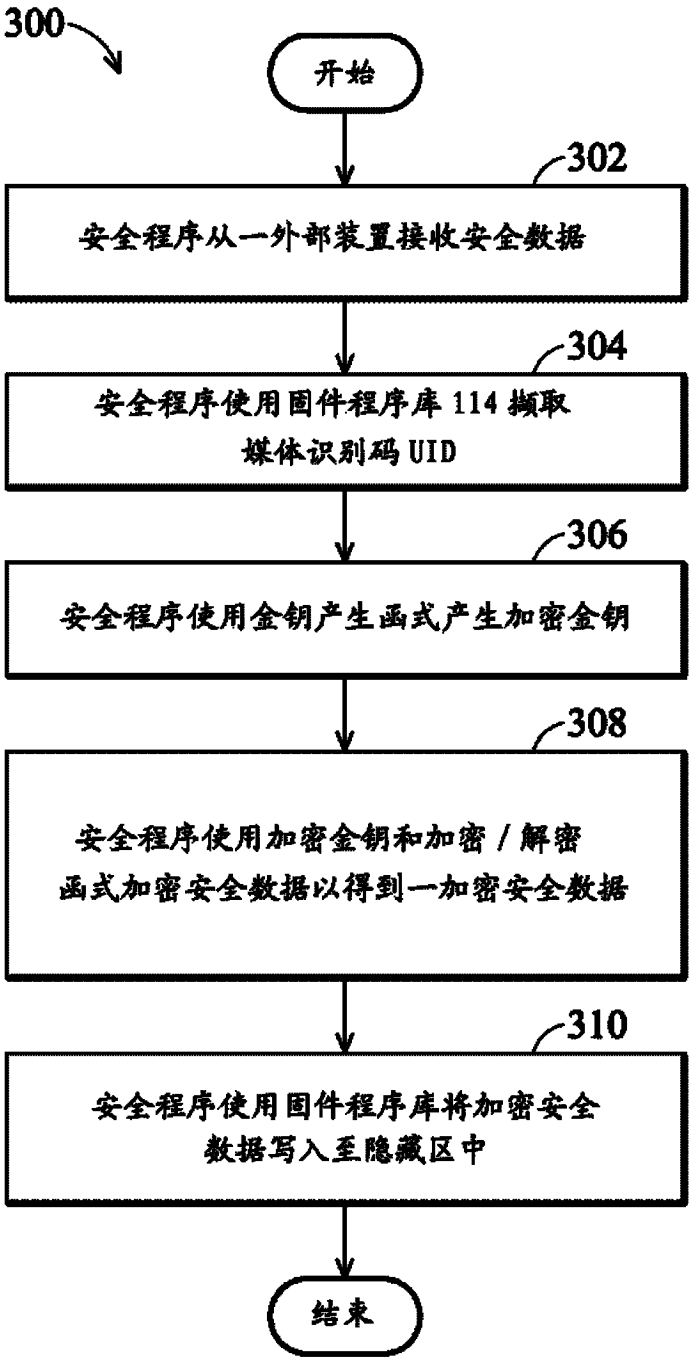

300
开始
302
安全程序从一外部装置接收安全数据
304
安全程序使用固件程序库 114 撷取
媒体识别码 UID
306
安全程序使用金钥产生函式产生加密金钥
308
安全程序使用加密金钥和加密 / 解密
函式加密安全数据以得到一加密安全数据
310
安全程序使用固件程序库将加密安全
数据写入至隐藏区中
结束

图 3A

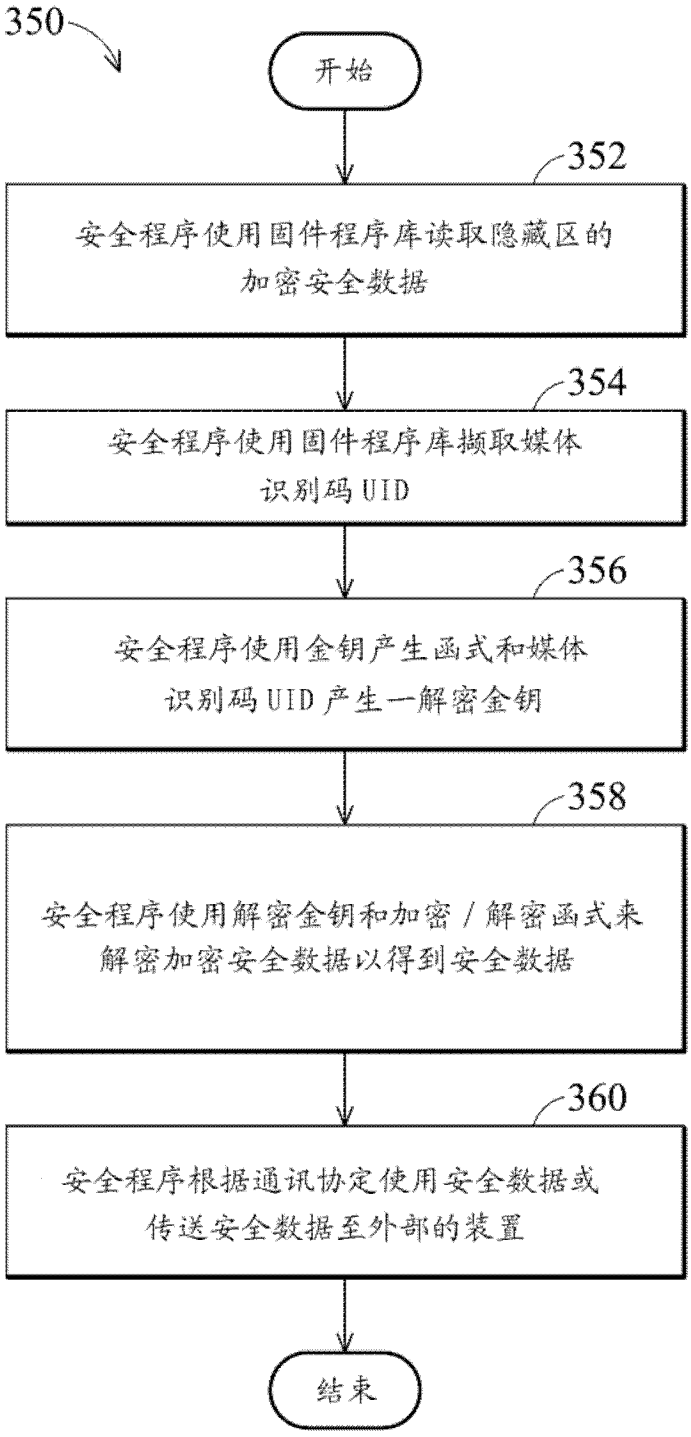

350
开始
352
安全程序使用固件程序库读取隐藏区的加密安全数据
354
安全程序使用固件程序库撷取媒体识别码 UID
356
安全程序使用金钥产生函式和媒体识别码 UID 产生一解密金钥
358
安全程序使用解密金钥和加密 / 解密函式来解密加密安全数据以得到安全数据
360
安全程序根据通讯协定使用安全数据或传送安全数据至外部的装置
结束

图 3B

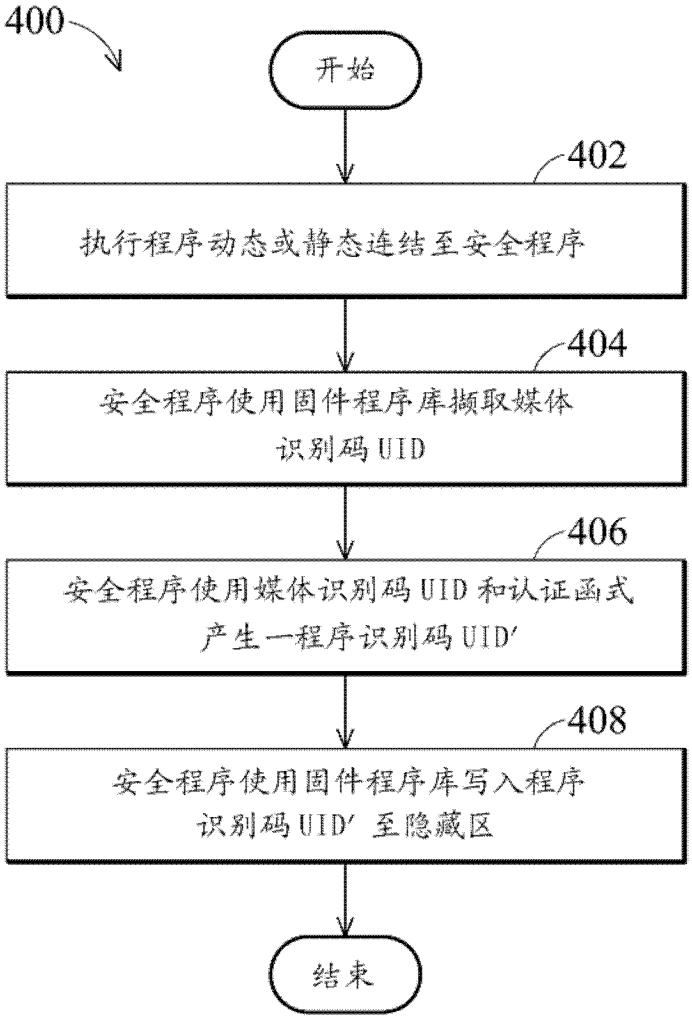

400
开始
402
执行程序动态或静态连结至安全程序
404
安全程序使用固件程序库撷取媒体识别码 UID
406
安全程序使用媒体识别码 UID 和认证函式产生一程序识别码 UID′
408
安全程序使用固件程序库写入程序识别码 UID′ 至隐藏区
结束

图 4A

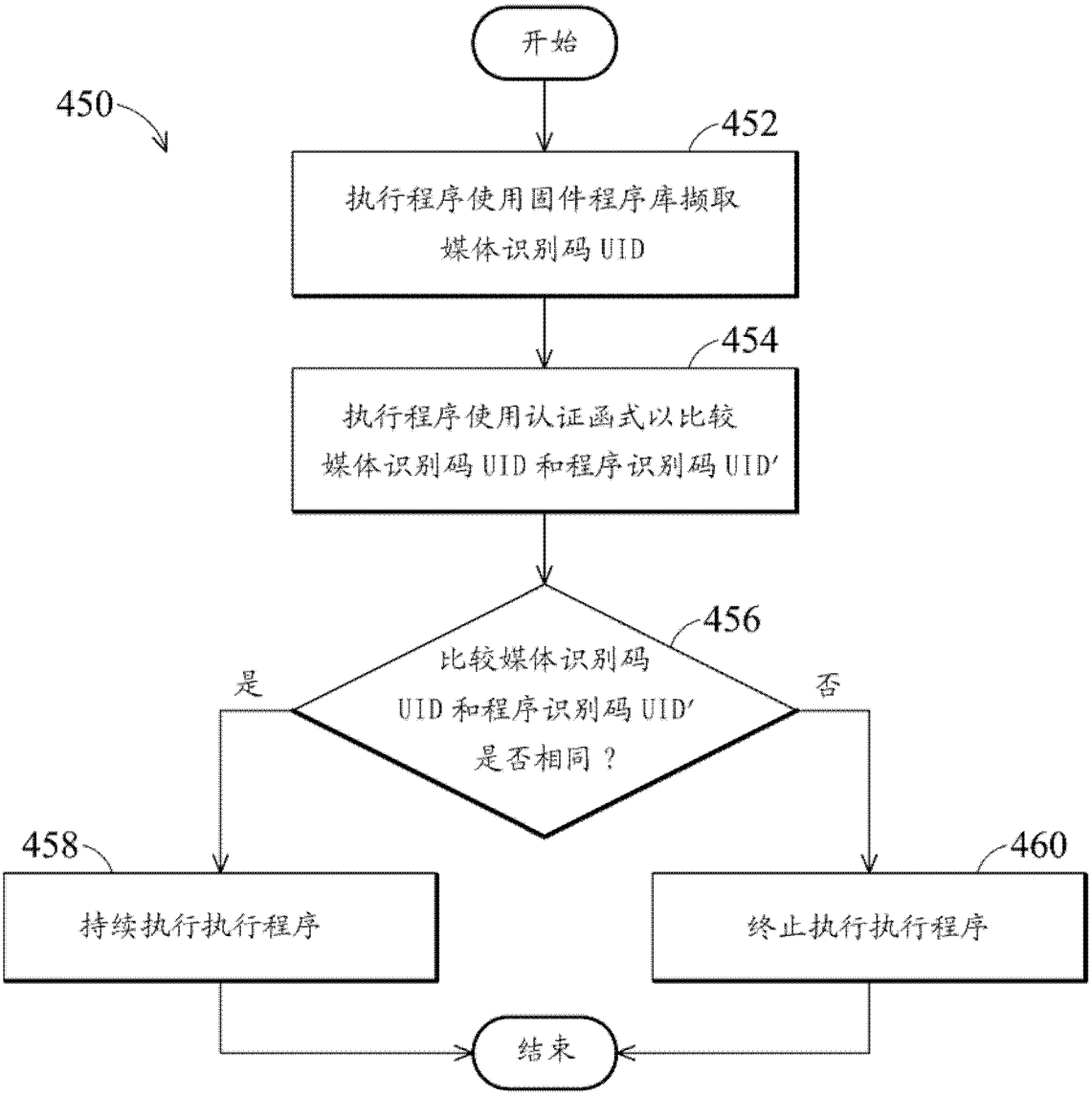

开始
450
452
执行程序使用固件程序库撷取
媒体识别码 UID
454
执行程序使用认证函式以比较
媒体识别码 UID 和程序识别码 UID′
456
比较媒体识别码
UID 和程序识别码 UID′
是否相同？
是
否
458
持续执行执行程序
460
终止执行执行程序
结束

图 4B

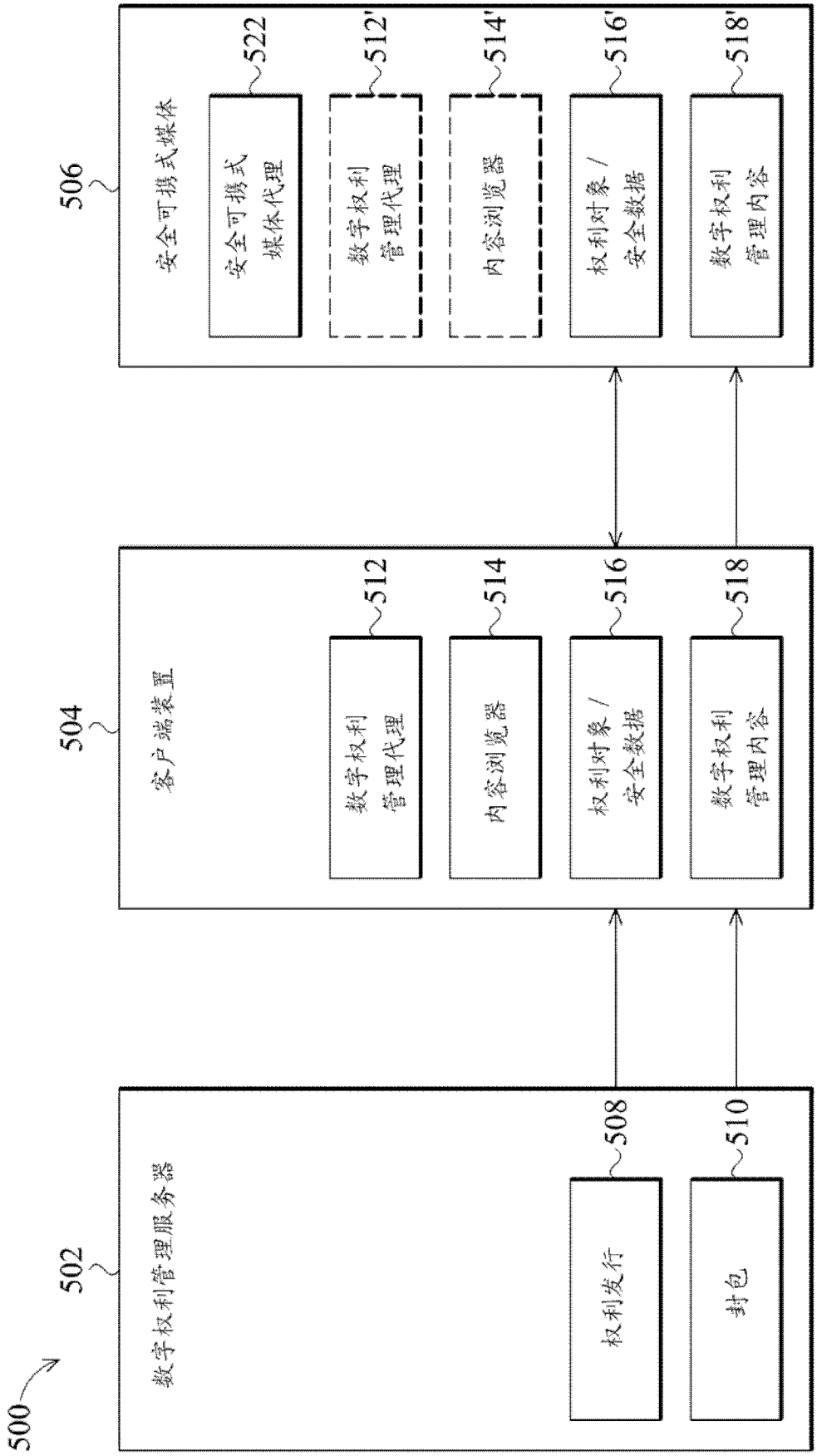

500
502
数字权利管理服务器
508
权利发行
510
封包
504
客户端装置
512
数字权利管理代理
514
内容浏览器
516
权利对象 / 安全数据
518
数字权利管理内容
506
安全可携式媒体
522
安全可携式媒体代理
512'
数字权利管理代理
514'
内容浏览器
516'
权利对象 / 安全数据
518'
数字权利管理内容

图 5

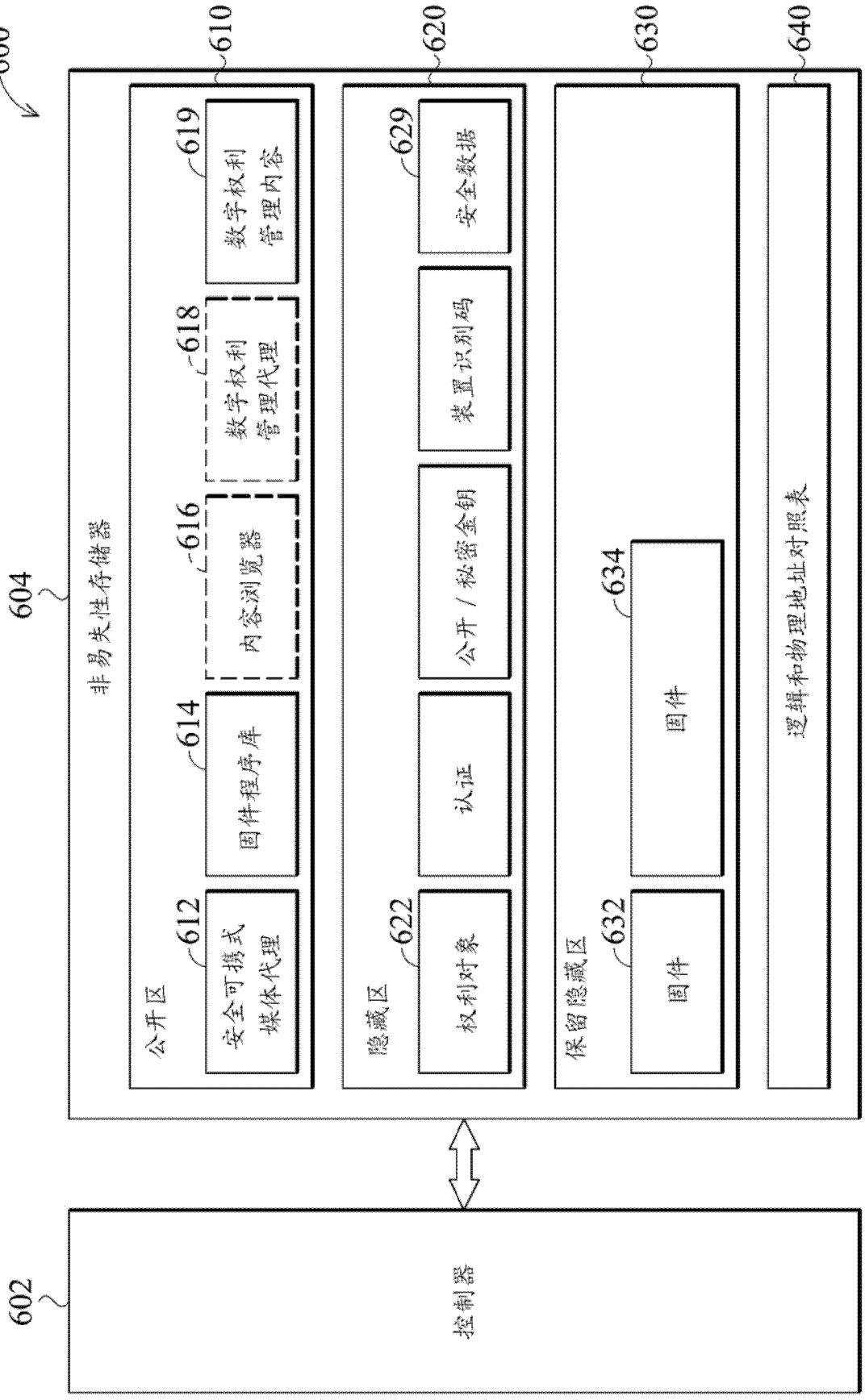

600
610
620
630
640
604
非易失性存储器
公开区
612
安全可携式媒体代理
614
固件程序库
616
内容浏览器
618
数字权利管理代理
619
数字权利管理内容
隐藏区
622
权利对象
认证
公开 / 秘密金钥
629
安全数据
装置识别码
保留隐藏区
632
固件
634
固件
逻辑和物理地址对照表
602
控制器

图 6

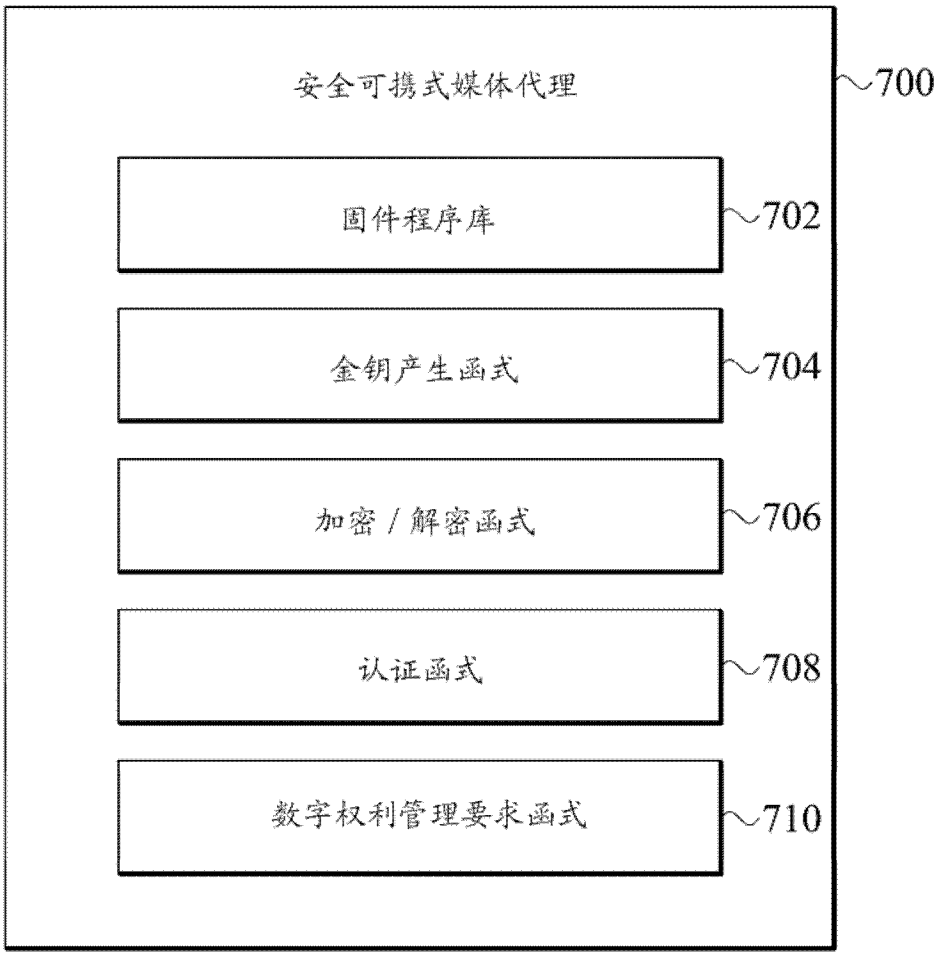

安全可携式媒体代理
700
固件程序库
702
金钥产生函式
704
加密 / 解密函式
706
认证函式
708
数字权利管理要求函式
710

图 7

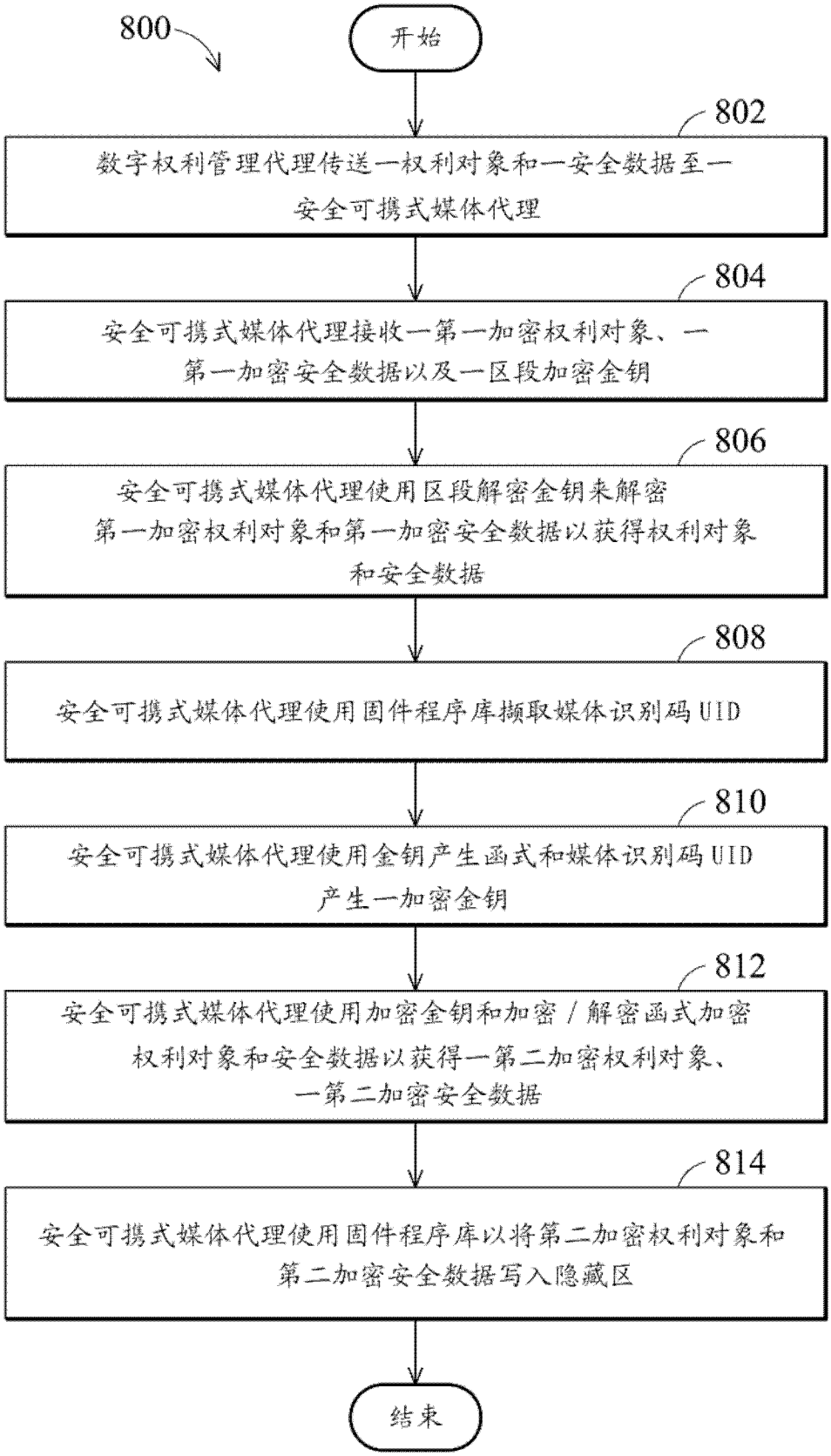

800
开始
802
数字权利管理代理传送一权利对象和一安全数据至一安全可携式媒体代理
804
安全可携式媒体代理接收一第一加密权利对象、一第一加密安全数据以及一区段加密金钥
806
安全可携式媒体代理使用区段解密金钥来解密第一加密权利对象和第一加密安全数据以获得权利对象和安全数据
808
安全可携式媒体代理使用固件程序库撷取媒体识别码 UID
810
安全可携式媒体代理使用金钥产生函式和媒体识别码 UID 产生一加密金钥
812
安全可携式媒体代理使用加密金钥和加密 / 解密函式加密权利对象和安全数据以获得一第二加密权利对象、一第二加密安全数据
814
安全可携式媒体代理使用固件程序库以将第二加密权利对象和第二加密安全数据写入隐藏区
结束

图 8A

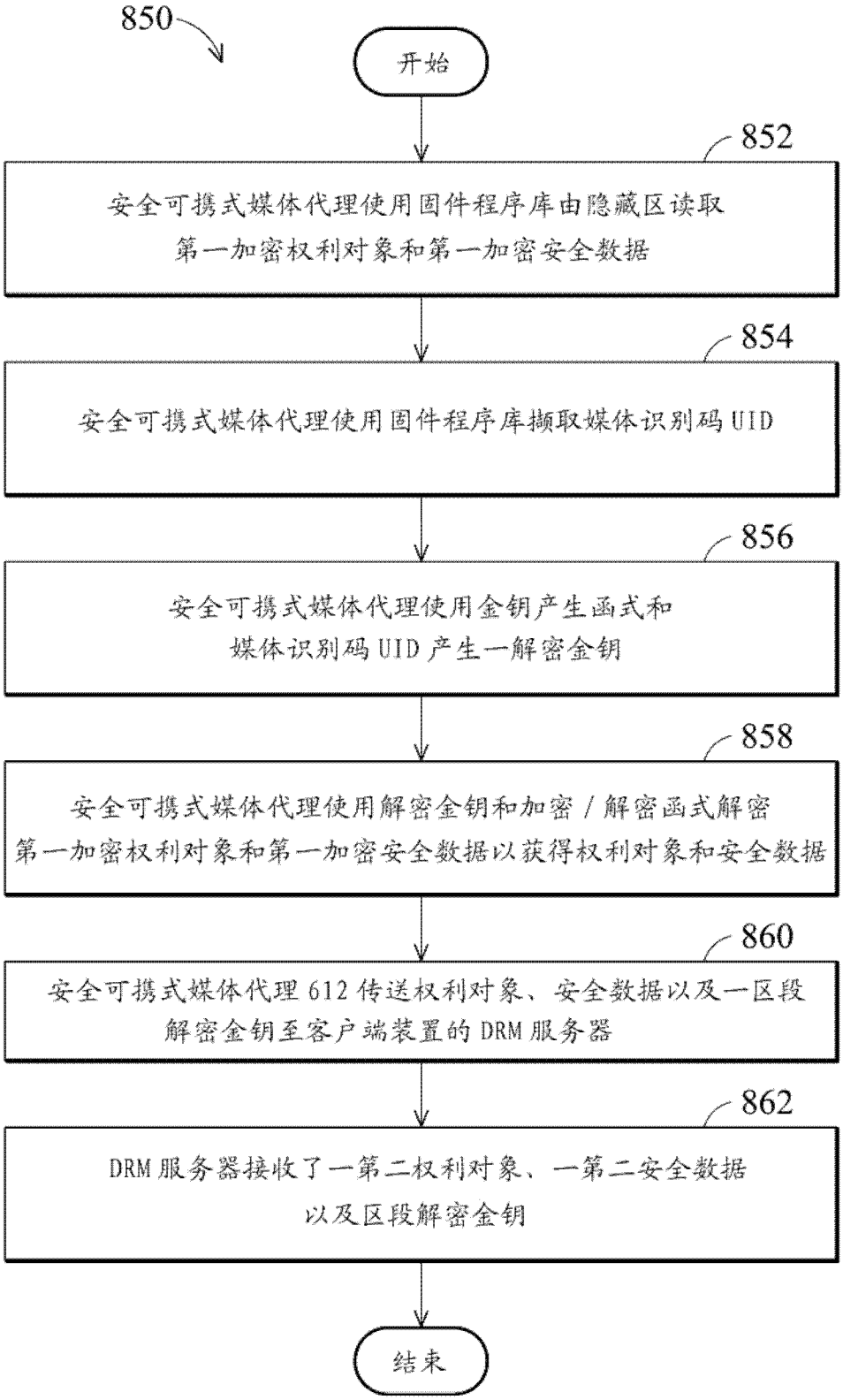

850
开始
852
安全可携式媒体代理使用固件程序库由隐藏区读取
第一加密权利对象和第一加密安全数据
854
安全可携式媒体代理使用固件程序库撷取媒体识别码 UID
856
安全可携式媒体代理使用金钥产生函式和
媒体识别码 UID 产生一解密金钥
858
安全可携式媒体代理使用解密金钥和加密 / 解密函式解密
第一加密权利对象和第一加密安全数据以获得权利对象和安全数据
860
安全可携式媒体代理 612 传送权利对象、安全数据以及一区段
解密金钥至客户端装置的 DRM 服务器
862
DRM 服务器接收了一第二权利对象、一第二安全数据
以及区段解密金钥
结束

图 8B


900
开始
901
安全可携式媒体代理使用固件程序库由一隐藏区读取
第一加密权利对象以及第一加密安全数据
902
安全可携式媒体代理使用固件程序库撷取一媒体识别码 UID
903
安全可携式媒体代理使用金钥产生函式以及
媒体识别码 UID 产生一解密金钥
904
安全可携式媒体代理使用解密金钥以及加密 / 解密函式
将第一加密权利对象以及第一加密安全数据解密以获得权利
对象和安全数据
905
安全可携式媒体代理传送权利对象、安全数据以及一区段
解密金钥至 DRM 代理
906
DRM 代理接收第二加密权利对象、第二加密安全数据
以及区段解密金钥
907
DRM 代理使用区段解密金钥将第二加密权利对象和
第二加密安全数据解密以获得权利对象和安全数据，且使用
获得的权利对象和安全数据来取得 DRM 内容
908
DRM 代理传送加密权利对象信息和区段解密金钥至
安全可携式媒体代理
909
安全可携式媒体代理使用区段解密金钥将加密权利对象信息解密
以获得权利对象信息
A

图 9A


A
910
安全可携式媒体代理使用固件程序库由隐藏区读取
第一加密权利对象和第一安全数据
911
安全可携式媒体代理使用固件程序库撷取媒体识别码 UID
912
安全可携式媒体代理使用金钥产生函式以及媒体识别码
UID 产生一解密金钥
913
安全可携式媒体代理使用解密金钥以及加密 / 解密函式将
第一加密权利对象以及第一加密安全数据解密以获得权利对象和
安全数据
914
安全可携式媒体代理使用权利对象信息来修正权利对象以
产生一修正的权利对象
915
安全可携式媒体代理使用固件程序库撷取媒体识别码 UID
916
安全可携式媒体代理使用金钥产生函式以及
媒体识别码 UID 产生一加密金钥
917
安全可携式媒体代理使用加密金钥以及加密 / 解密函式将
修正的权利对象和安全数据加密以取得第三加密权利对象以及
第三加密安全数据
918
安全可携式媒体代理使用固件程序库将第三加密权利对象以及
第三加密安全数据写入隐藏区中
结束

图 9B