



## [12] 发明专利申请公布说明书

[21] 申请号 200880013343.4

[43] 公开日 2010年3月10日

[11] 公开号 CN 101669124A

[22] 申请日 2008.6.26

[21] 申请号 200880013343.4

[30] 优先权

[32] 2007.6.29 [33] US [31] 11/771,804

[86] 国际申请 PCT/US2008/008019 2008.6.26

[87] 国际公布 WO2009/005719 英 2009.1.8

[85] 进入国家阶段日期 2009.10.23

[71] 申请人 桑迪士克公司

地址 美国加利福尼亚州

[72] 发明人 罗伯特·C·常 袁 珀

巴曼·卡瓦米

法西德·萨比特-沙吉 王军志

刘宪军 杨奇浩 琼·李 严 梅

法布里斯·乔甘德-库伦布

[74] 专利代理机构 北京市柳沈律师事务所

代理人 黄小临

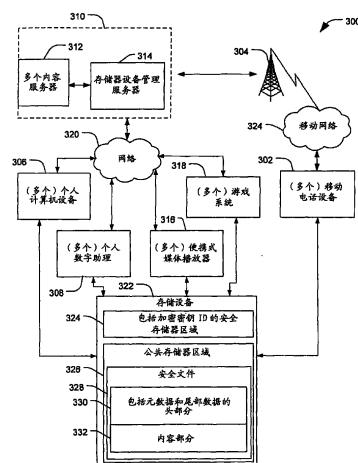
权利要求书3页 说明书20页 附图8页

## [54] 发明名称

从存储器存储和访问头数据的方法

## [57] 摘要

公开了使用文件的头部分存储和访问数据的方法。在实施例中，公开了一种在非易失性存储器中存储内容的方法。该方法包括读取包括媒体内容且包括尾部的内容文件，在文件的头部中存储与该尾部相关的信息以及安全数据；以及将该文件存储到该非易失性存储器或耦合于该非易失性存储器设备的主机设备的存储器区域的存储元件。



1. 一种在非易失性存储器中存储内容的方法，该方法包括：

读取包括媒体内容且包括尾部的内容文件，该尾部包括与该内容相关的尾部数据；

在文件的头部分中存储与该尾部数据相关的信息以及安全数据；以及

将该文件存储到该非易失性存储器和耦合于该非易失性存储器设备的主机设备的存储器区域中的至少一个的存储元件。

2. 根据权利要求 1 的方法，其中，所述头部分包括元数据，该元数据包括 ID3 数据。

3. 根据权利要求 1 的方法，其中，结合在所述安全文件的头部分中存储尾部数据以及安全数据，使用应用编程接口（API）。

4. 根据权利要求 1 的方法，其中，所述信息包括尾部数据位置信息。

5. 根据权利要求 1 的方法，其中，所述安全数据包括与用于加密来自所述内容文件的媒体内容的加密密钥相关联的至少一个加密 ID。

6. 根据权利要求 1 的方法，还包括经由数据下载处理来从外部系统接收所述内容文件。

7. 根据权利要求 1 的方法，其中在将所述非易失性存储器设备分发给消费者之前在所述非易失性存储器设备中存储所述媒体内容。

8. 一种提取内容的方法，该方法包括：

从非易失性存储器读取内容；

从文件的一部分读取与该内容相关联的尾部数据信息，该部分还包括与该内容相关的安全数据项；以及

向具有对所述非易失性存储器的访问的主机设备的显示设备提供该尾部数据信息。

9. 根据权利要求 8 的方法，其中，所述主机设备访问来读取所述内容以供回放。

10. 根据权利要求 8 的方法，其中，所述内容包括音频数据和视频数据。

11. 根据权利要求 8 的方法，其中结合从所述文件读取所述尾部数据信息，使用应用编程接口（API），且其中，所述主机设备将文件名和元数据结构传递给文件系统工具包，且其中，所述文件系统工具包使用所述 API 来将

元数据写入该文件。

12. 一种使用非易失性可重写存储器来访问媒体内容的方法，该方法包括：

接收关于访问权限的信息；

在非易失性可重写存储器的安全存储器区域中存储所述访问权限，所述访问权限允许对用于解密被存储在非易失性可重写存储器中的加密媒体内容的内容解密密钥的访问；

供应至少一个所选的加密媒体内容项的解密版本；以及

供应从安全存储器区域的头部分提取的元数据，该元数据与至少一个所选的加密媒体内容项相关联，所述至少一个所选的加密媒体内容项的解密版本要被提供给主机设备。

13. 根据权利要求 12 的方法，还包括接收验证信息，且在接收该验证信息之后使用该内容解密密钥来解密所述至少一个所选的加密媒体内容项。

14. 根据权利要求 12 的方法，其中，所述主机设备包括用于呈现所述至少一个所选的加密媒体内容项的解密版本的回放设备，该方法还包括：

将所述主机设备连接到服务器；

从所述主机设备向所述服务器发送购买授权；

在所述主机设备接收关于所述验证信息和所述访问权限的信息；以及向所述非易失性可重写存储器供应所述验证信息和所述访问权限。

15. 根据权利要求 12 的方法，其中，所述主机设备是电话设备、个人数字助理（PDA）、和计算机中的一个。

16. 根据权利要求 12 的方法，其中，所述元数据包括艺术家名、艺术家名的长度、内容名、内容名的长度、专辑名、专辑名的长度或其任意组合。

17. 根据权利要求 12 的方法，还包括响应于接收到验证信息更改访问权限来提供对所述内容解密密钥的访问，以便允许对被存储在所述非易失性可重写存储器中的所选的加密媒体内容的访问。

18. 根据权利要求 17 的方法，还包括将所述主机设备连接到服务提供者；从所述主机设备向该服务器提供者发送购买权限；以及从该服务提供者接收所述验证信息和用于更改所述访问权限的信息。

19. 根据权利要求 12 的方法，还包括显示与该元数据相关的信息。

20. 根据权利要求 12 的方法，还包括呈现所述至少一个所选的加密媒体

内容项的解密版本，而同时显示与该元数据相关的信息。

21. 一种在非易失性存储器中存储内容的方法，该方法包括：

读取包括媒体内容且包括尾部的内容文件，该尾部包括与该内容相关的尾部数据；

在文件中存储与尾部数据相关的信息以及安全数据；以及

将该文件存储到该非易失性存储器和耦合于该非易失性存储器设备的主机设备的存储器区域中的至少一个的存储元件。

## 从存储器存储和访问头数据的方法

### 背景技术

本公开通常涉及包括对文件的头部分和内容部分的访问的非易失性存储器系统。包括非易失性存储器设备的诸如存储卡的存储器系统有很多目的，且可以被用于存储媒体内容，诸如音频或视频文件。在这种系统中，关于媒体内容的信息，诸如歌曲或电影的题目，可以被存储在存储器的最后扇区中。存储器系统的主机设备，诸如移动电话或主机计算机，可能需要针对多个数据文件检索文件的最后扇区，且在主机设备处的文件系统可以被要求遍历存储器簇来找到与该多个数据文件中的一个或多个相关联的最后扇区数据。这个任务可能消耗相当大量的宝贵处理资源，并花费大量的时间，从而降低了设备的性能。例如，在初始化处理器期间，可能请求处理器来遍历(traverse)具有上千文件的文件访问表(file access table, FAT)，由此导致初始化时段延长，这引起感受到性能降低。另外，对于媒体文件，消费者可能想要找到音乐信息供显示。在媒体文件开始播放之前，传统的系统可能花费长时间来读取指定的扇区，并查看该帧。对于特定处理器以及对于包含大量加密文件的存储器，这个问题可能更严重。因此，需要对存储的媒体内容的改进控制。

### 附图说明

图 1 是包括主机设备和存储器设备的系统的示例实施例的方框图。

图 2 是图示用于与所耦合的主机设备和存储器设备一起使用的控制器的具体实施例的方框图。

图 3 是图示了图 1 的系统的应用的总体图。

图 4 是图示了存储内容文件的方法的具体实施例的流程图。

图 5 是图示了从存储器提取内容的方法的具体实施例的流程图。

图 6 是图示了读取和呈现(render)内容文件的内容的方法的具体实施例的流程图。

图 7 是图示可以被存储在计算机可读介质中的安全文件的数据结构的总体图。

图 8 是图示可以被存储在计算机可读介质中的安全文件的头部分的数据结构的总体图。

图 9 是图示可以被存储在文件的头部分中的元数据的数据结构的总体图。

图 10 是图示可以被存储在文件的头部分中的尾部(trailer)的数据结构的总体图。

### 发明内容

公开了使用文件的头部分来存储和访问数据的方法。在实施例中，公开了一种在非易失性存储器中存储内容的方法。该方法包括：读取包括媒体内容且包括尾部的内容文件，在文件的头部分中与安全数据一起存储与尾部相关的信息，并将该文件存储到非易失性存储器的存储元件或耦合于该非易失性存储器设备的主机设备的存储器区域。该信息可能包括尾部位置。

在另一个实施例中，公开了一种提取内容的方法。该方法包括从非易失性存储器读取内容，从安全文件的头部分读取与该内容相关的尾部数据信息，并向访问该非易失性存储器的主机设备的显示设备提供与尾部数据相关的数据。该头部分还包括与内容相关的安全数据。

在另一实施例中，公开了一种通过使用非易失性可重写存储器来访问媒体内容的方法。该方法包括接收关于访问权限的信息，在非易失性可重写存储器的安全存储器区域中存储该访问权限，供应至少一个选择的加密媒体内容项的解密版本，并供应从安全存储器区域的头部分提取的元数据。该元数据与该至少一个选择的加密媒体内容项相关联。要向主机设备提供该至少一个选择的加密媒体内容项的解密版本。该访问权限允许访问用于解密在非易失性可重写的存储器中存储的加密媒体内容的内容解密密钥。

### 具体实施方式

图 1 是包括主机设备 102 和主机设备 102 可访问的存储器设备 110 的系统 100 的图示实施例的方框图。虽然在主机设备 102 中图示存储器设备 110，但是存储器设备 110 可以是主机设备 102 可经由一个或多个接口访问的外部存储器设备，该一个或多个接口诸如为通用串行总线(USB)接口、小计算机系统接口(SCSI)、先进技术附接(AT)、集成驱动电子(IDE)接口、串

行 ATA 接口、火线 (FireWire) 接口、其他接口或其任意组合。在具体示例实施例中，存储器设备 110 可以是闪存卡、智能卡、硬盘、另一存储器类型或其任意组合。

主机设备 102 可以经由网络 104 与服务提供者 106 通信。服务提供者 106 可以是媒体内容源。该主机设备还可以将显示数据传送给显示设备 108，该显示设备 108 可以被耦合于主机设备 102 或与主机设备 102 集成。

主机设备 102 包括存储器设备 110、访问存储器设备 110 的处理器 112、显示接口 116、和响应于网络 104 的网络接口 114。显示接口 116 可以从处理器 112 接收数据，并向显示设备 108 传送数据以显示。存储器设备 110 包括存储介质 118 和控制对在存储介质 118 存储的数据的访问的控制器 120。存储介质 118 包括安全存储器区域 122 和公共存储器区域 124。安全存储器区域 122 包括加密密钥标识符 (ID) 126、一个或多个控制结构 128 和可选地具有加密密钥表 130。

公共存储器区域 124 也可以包括安全文件 132，该安全文件 132 包含具有元数据和尾部数据的头部分 144 且包括内容部分 146。头部分 144 包括安全数据、尾部数据和与要被存储在公共存储器区域 124 中的内容相关的元数据。安全数据可以包括与在存储介质 118 的安全存储器区域 122 中的隐藏区域相关的目录信息。尾部数据可以包括与文件内容的预定部分相关联的位置。例如，尾部数据可以包括与内容的限制部分，诸如文件的最后 512 字节、来自文件的数据的选择扇区、文件的预定段、或其任意组合，相关联的位置。在具体示例实施例中，尾部数据包括指示尾部数据是否与扇区边界对齐的第一字段、标识尾部数据的扇区数的第二字段、标识尾部数据的扇区偏移值的第三字段、和标识与存储器设备 110 的存储器区域、诸如安全存储器区域 122 和公共存储器区域 124 的扇区相关联的字节偏移值的第四字段。头部分 144 包括至少一个安全数据项，且包括与要被存储在非易失性存储器、诸如存储器设备 118 中的媒体内容相关的元数据。头部分 144 可以包括可变数量的字段，该可变数量的字段包括与内容文件相关的数据。至少一个字段包含签名区域。

主机设备 102 包括软件驱动器 134，软件驱动器 134 可以由处理器 112 执行，以与主机设备 102 的各个组件，诸如显示接口 116、网络接口适配器（诸如网络接口适配器 114）、调制解调器、其他内部和外围硬件、或其任意

组合来通信。另外，主机设备 102 包括可以由处理器 112 执行以向主机设备 102 提供功能的软件应用 136 和应用编程接口（API）138。API 138 可以包括可由处理器执行以在文件的头部分中存储要被存储在存储器设备 110 中的文件的最后扇区位置（例如，尾部数据）的一个或多个指令。API 138 还可以包括用于读取文件的最后扇区的至少一个指令。

主机设备 102 还包括系统代理/文件系统工具包 140。系统代理/文件系统工具包 140 包括可以由处理器 112 或由控制器 120 执行以配置存储介质 118 的各个方面的系统代理软件应用。系统代理/文件系统工具包 140 可以被用于基于与系统代理/文件系统工具包 140 相关联的一组证书(credential)来访问存储在存储介质 118 上的内容。在特定实施例中，系统代理/文件系统工具包 140 可以具有内置的一组证书，该内置的一组证书可以由控制器 120 使用在存储介质 118 的隐藏分区 148 中存储的访问控制记录 150 来验证。

另外，主机设备 102 包括可由处理器 112 和/或控制器 120 执行以访问安全存储器区域 122 和公共存储器区域 124 的读/写应用。存储器设备 110 还可以包括隐藏分区 148。该隐藏分区 148 可能对于主机设备 102 的文件系统不可见，但可以被存储器设备 110 的控制器 120 访问。隐藏分区 148 可以包括一个或多个访问控制记录（Access Control Record, ACR）150。每个记录可以包括验证证书和相关联的许可的表。控制器 120 可以使用在隐藏分区 148 中的 ACR 150 来通过验证每个访问请求和每个主机应用来控制对被存储在公共存储器区域 124 中的内容和对安全存储器区域 122 的访问。在具体示例实施例中，主机设备 102 可以与控制器 120 建立安全会话，且控制器 120 可以解密来自安全存储器区域 122 的内容，并在向主机设备 102 提供该内容之前使用会话密钥来加密内容。以此方式，保护内容，且可以由控制器 120 使用加密密钥，而不将加密密钥暴露于存储器设备 110 之外。

通常，为了访问隐藏分区 148，提供对访问控制记录（ACR）的登录。在登录之后，控制器 120 可以提取内容。在具体示例实施例中，可以基于登录来提取访问许可以提供对所提取内容的不受限的回放。在另一具体示例实施例中，可以从内容标识符和秘密值（诸如在主机设备 102 和存储器设备 110 之间共享的秘密值）来计算登录。具有系统代理/文件系统工具包 140 的主机设备 102 由于工具包内置于正确的证书而可以访问内容。

在具体示例实施例中，存储器设备 110 包括可以结合在主机设备 102 中

运行的应用而使用的受信的(trusted)内容保护特征。应用可以包括可以是应用的部分的数字权限管理代理。例如，应用可以是媒体内容播放器应用，诸如MP3播放器应用，其可以包括数字权限管理（DRM）代理。对存储在存储器设备110上的内容的访问可以通过登录到访问控制记录150中来控制，该访问控制记录150可以存储在存储器设备110的存储介质118的隐藏分区148中。访问控制记录150可以包括多个受信标识符和相关联证书。

在具体示例实施例中，隐藏分区148可以包括一组访问控制记录150。例如，在主机设备102上运行的每个应用可以具有其自身的数字权限管理代理，且隐藏分区148可以包括与每个数字权限管理（DRM）代理相关联的访问控制记录150。在替换的实施例中，隐藏分区可以包括访问权限管理表。访问控制记录（ACR）150可以被用于建立在存储器设备110和在主机设备102上运行的应用之间的安全会话。ACR 150还可以被用于确定访问许可，以控制对所存储内容的访问。

在具体示例例子中，该文件的内容部分可以包括音频数据、诸如歌曲，且针对该文件的元数据可以包括指示与音频数据相关联的相关歌曲信息，诸如标题、具体音轨的长度、表演者的姓名、其他信息，或其任意组合的数据。在具体示例实施例中，相关歌曲信息可以包括标识信息，诸如运动图像专家组（MPEG）音频层-3（MP3）标识信息。

安全存储器区域122可以接收和存储控制结构128和其他安全数据，诸如加密密钥标识符（ID）126。可以访问加密密钥ID 126以找到(locate)可用于加密或解密媒体内容项的加密密钥。

在具体示例实施例中，可以由制造者、服务提供者、转售者、或另一资源提供存储器设备110。存储器设备110可以包括预装载的媒体内容、诸如音频内容、视频内容、其他媒体内容，或其任意组合。控制器120可以使用在隐藏分区148中的ACR来验证主机设备102并确定用于与主机设备102一起使用的访问许可。一旦确定了这种访问许可，控制器120可以使用软件API 138和读/写应用142来控制对这种预装载的媒体内容的访问。例如，API 138可以包括权限管理协议，控制器120可以使用该权限管理协议来将媒体内容锁定于存储器设备110。API 138可以允许媒体内容在支持设备、诸如主机设备102上播放。另外，如果存储器设备110是可移除存储器设备，诸如闪存卡，则可以把存储器设备110移除并连接到可用于访问和播放媒体内容的不

同回放设备。通过向内容文件的头部分中插入元数据，媒体回放设备可以容易地访问例如标题、歌曲信息以产生供用户选择的播放列表。

在具体示例实施例中，主机设备 102 可以把来自文件访问表 (FAT) 的文件和存储器地址提供给存储设备 110 以供安全存储。可以由主机设备 102 维持和控制 FAT。主机设备 102 还可以向存储设备 110 提供加密密钥标识符 (ID)。控制器 120 可以执行一个或多个 API 138 和读/写应用 142 来从文件的内容抽取元数据和与尾部数据相关的位置信息，并把所抽取的元数据和位置信息插入到文件的头部分中。或者，可以从文件的内容抽取尾部数据，并将其插入头部分。此外，控制器 120 可以把来自安全文件 132 的头部分 144 的安全数据写到安全存储器区域 122。控制器 120 还可以访问加密密钥表 130 以提取与加密密钥 ID 相关联的加密密钥。或者，控制器 120 可以生成加密密钥、在加密密钥表 130 中存储加密密钥、在加密密钥 ID 126 中存储加密密钥 ID、且存储在加密密钥 ID 和加密密钥表 130 之间的关联。控制器 120 可以使用加密密钥来加密文件。然后，该加密的文件可以被存储在公共存储器区域 124 中作为安全文件 132。

通常，系统代理/文件系统工具包 140 可以与多个不同存储器设备结合来使用。API 138 允许用户来访问包括安全文件 132 的头部分 144 的数据。公开的系统和方法扩展头的使用来存储信息来增强性能，以提供与内容相关的信息；或用于其他目的。例如，元数据和与尾部数据相关的位置信息可以被存储在头部分 144 中，以提供对来自安全文件 144 的文件内容的受限数据的迅速(really)访问，而无需必须解密整个安全文件。受限数据可以包括诸如媒体内容标题、作者、长度、文件类型、预览数据、其他信息或其任意组合的信息。

在具体示例实施例中，存储器设备 110 可以包括可由控制器 120 执行以请求文件系统来在头中存储最后扇区位置的 API 138。另一 API 138 可以由控制器 120 执行来读取存储介质 118 的一部分的最后扇区。对于预装载文件，系统代理/文件系统工具包 140 可以包括通过抽取例如 MP3 歌曲的 ID3 信息来建立与文件内容相关的元数据文件的功用。系统代理/文件系统工具包 140 可以被用来通过将元数据写入包括预装载的媒体内容（例如音频内容、视频内容、其他内容或其任意组合）的文件的头部分中来建立预装载的存储卡。这种预装载的存储卡的例子是在商业上可从加州的 Milpitas 的 SanDisk 公司

可得到的 GRUVI 卡。

通常，API 138 可以由控制器 120 执行来进行各种 API 功能。可用的 API 的例子包括存储元数据的 API、提取元数据的 API、存储与尾部数据相关的位置信息或尾部数据的 API、和提取尾部数据的 API。存储元数据的 API 具有要存储的元数据的数据结构和文件名的输入。主机设备 102 将文件名和元数据结构传递到已由控制器 120 装载的系统代理/文件系统工具包 140。系统代理/文件系统工具包 140 将元数据写入文件的头部分以存储。在具体实施例中，元数据结构和元数据信息包括如下的一个或多个：内容名、艺术家名、专辑名、流派、持续时间、版权、内容的描述、帧数、时间、比特率、采样率和立体声指示符。

API 138 还包括“提取元数据” API，该“提取元数据” API 以文件名和元数据结构作为其输入。提取元数据 API 提供指示成功或错误的状态作为其输出。提取元数据 API 被用于提取并填充元数据结构。提取元数据 API 由主机设备 102 使用，该主机设备 102 将文件名和空元数据结构传递到系统代理/文件系统工具包 140。系统代理/文件系统工具包 140 从所存储的安全文件 132 的头部分 144 填充元数据结构。

API 138 还可以包括“存储尾部数据” API，该“存储尾部数据” API 接收文件名作为其输入。存储尾部数据 API 提供指示存储操作成功或存储操作遭遇错误的状态输出。存储尾部数据 API 可以提供成功码或错误码作为其输出。存储尾部数据 API 被主机设备 102 使用，该主机设备 102 将文件名传递到系统代理/文件系统工具包 140。系统代理/文件系统工具包 140 从目录条目提取所存储的文件信息，并确定文件的最后扇区位置。然后，存储尾部数据 API 填充尾部框并将尾部数据写入头。

API 138 还可以包括“提取尾部数据” API，该“提取尾部数据” API 以文件名、缓冲器示出和缓冲器作为其输入。提取尾部数据 API 提供状态指示符作为其输出。提取尾部数据 API 在成功时填充缓冲器，并提供在缓冲器中的数据的长度。在使用提取尾部数据 API 期间，主机设备 102 将文件名传递到系统代理/文件系统工具包 140。系统代理/文件系统工具包 140 读取头部分 144 的尾部数据并从目录条目提取文件信息。然后，提取尾部数据 API 检查安全文件 132 是否已经被修改或移动了。如果文件信息匹配头，则提取尾部数据 API 使用该信息来读取尾部数据。然后，提取尾部数据 API 填充缓冲器

直至缓冲器尺寸，且将填充后的缓冲器返回到主机设备。如果由于尺寸限制因此存在比将适合(fit in)缓冲器更多的数据，则提取尾部数据 API 返回指示缓冲器对于所有尾部数据太小的状态。用户、主机设备 102、或控制器 120 可以使用系统代理/文件系统工具包 140 和上述 API 138 来将内容存储到安全存储器区域 122 或提取先前所存储的内容。另外，在主机设备上运行的应用可以使用 API 138 来提取所请求的内容以回放。

内容文件可以包括音频内容、视频内容、文本数据、多媒体内容、其他数据内容或其任意组合。主机设备 102 的处理器 112 可以执行软件 136 和读/写应用 142 来从内容文件读取内容并回放。在具体示例实施例中，存储器设备 110 适于管理加密密钥，而不向外部组件提供加密密钥。存储器设备 110 可以适于使用由主机设备 102 提供或从其他设备接收的加密密钥标识符来找到与所选的媒体内容相关联的密钥，并管理在存储器设备 110 中的加密/解密。

在具体示例实施例中，主机设备 102 可以经由网络 104 与在服务提供者 106 处的服务器通信。在具体实施例中，网络 104 可以是局域网。在另一具体实施例中，网络 104 可以是广域网，诸如因特网。在服务提供者 106 处的服务器可以向主机设备 102 提供媒体内容，且可以与控制器 120 和/或系统代理/文件系统工具包 140 通信来生成在存储介质 118 的安全存储器区域 122 中的控制结构 128。控制器 120 可以利用控制结构 128 来管理和控制对存储在存储介质 118 处的具体媒体内容的访问。

在示例例子中，安全文件 132 的内容部分 146 包括视频数据。头部分 144 具有与尾部数据相关的位置信息，该尾部数据包括与被存储在安全文件 132 的预定位置中的视频数据相关的信息。例如，尾部数据可以包括来自文件的结尾、来自文件的最后扇区或最后数据块、来自文件的预定部分、来自文件的多个部分、或其任意组合的数据。头部分 144 可以包括与文件的结尾、文件的最后扇区或最后数据块等相关的位置信息。可以向主机设备 102 提供视频数据用于经由显示设备 108 来回放和显示，该显示设备 108 可以包括音频再现能力。处理器 112 可以向显示设备 108 提供与尾部数据相关的数据，同时在存储器设备 110 处进行验证，同时在存储器设备 110 处解密安全文件 132，或其任意组合。

在具体示例实施例中，主机设备 102 可以包括系统代理/文件系统工具包，诸如系统代理/文件系统工具包 140，用于提供对加密计算机可读文件的读和

写访问。主机设备 102 的处理器 112 可以利用系统代理/文件系统工具包 140 来在内容文件的头部分中存储与来自内容文件的最后扇区的尾部数据相关的位置信息。然后，修改的内容文件可以被加密和被存储在公共存储器区域 124 中，作为安全文件 132。在稍后，主机设备 102 的处理器 112 可以读取安全文件 132 的头部分 144 来获得与内容 146 相关的数据。处理器 112 可以经由显示接口 116 向显示设备 108 提供与头部分 144 相关的数据，诸如元数据。处理器 112 还可以向控制器 120 提供加密密钥 ID，该控制器 120 可以利用安全存储器区域 122 的加密密钥 ID 126 来标识解密密钥，并解密安全文件的内容部分 146，并向处理器 112 提供解密的内容。通常，在从公共（第二）存储器区域 124 回放内容之前或期间，处理器 112 可以向显示设备 108 提供来自头部分 144 的与该数据相关的信息。

通常，诸如存储器设备 110 的非易失性可重写存储器设备特别适用于存储媒体内容。例如，闪存卡具有可以用于存储包括电影、视频游戏、音频数据或其任意组合的媒体内容的大存储容量。另外，由于闪存卡可重写，所以相比于诸如光盘的高容量非可重写存储器，这种存储器设备更灵活。一旦在非易失性可重写存储器设备中的媒体内容可以由内容所有者或代表内容所有者、诸如版权所有者、内容提供者、服务提供者 106、另一实体或其任意组合安全保护并控制，则具有用于分发媒体内容的新方法。然后，终端用户将能够通过不同主机设备来访问在这种存储器设备中的媒体内容，而无需必须订阅多个媒体服务。诸如服务提供者 106 的服务提供者还可以通过能够针对安全地存储媒体内容并以受控方式分发媒体内容的服务收费而得到另外的收入。

例如，非易失性可重写存储器设备、诸如存储器设备 110 可能预装载有包括加密媒体内容和与加密媒体内容相关的数据的数据。在具体示例实施例中，与加密媒体内容相关的数据可以包括预览数据，诸如加密媒体内容的未加密部分或这种媒体内容的未加密较低质量版本。预览数据还可以包括限制播放次数或呈现全长媒体内容的指令。

在具体示例实施例中，服务提供者 106 可以向主机设备 102 提供媒体内容，包括具有回放限制的预览数据。内容提供者 106 可以包括可以经由网络 104 提供可由主机设备 102 访问的用户接口来购买对加密媒体内容的不受限访问权限的一个或多个服务器。终端用户购买对访问加密媒体标题的权限之

后，服务提供者 106 可以向主机设备 102 提供密钥、控制结构或其他数据，用于由控制器 120 使用来提供对媒体内容的访问。在该示例实施例中，与主机设备 102 相关联的信息可以包括证书、证明、其他类型的验证信息、或其任意组合。与主机设备 102 相关联的信息还可以包括关于访问权限、访问规则、回放规则、媒体内容共享限制、和/或媒体内容复制限制的信息来控制对可用于预览的加密媒体内容的访问。与预览数据相关联的加密媒体内容仅在购买之后变为可用于终端用户。在具体实施例中，在购买之后，服务提供者 106 可以向主机设备 102 传送加密媒体内容的未删节版本。在另一具体实施例中，在购买之后，服务提供者 106 可以向主机设备 102 传送解密密钥，来允许主机设备 102 解密预装载的加密媒体内容。

在替换实施例中，加密媒体内容可以被预装载到上述非易失性可重写存储器设备 106。另外，访问信息、包括访问权限、访问规则、回放规则、其他控制信息、或其任意组合可以被预装载到存储器设备 110 中。控制器 120 可以使用这种访问信息来控制对媒体内容的访问。该访问信息可以指定仅加密媒体内容的选择部分、这种媒体内容的较低质量版本、与媒体内容相关的文本数据、其他数据、或其任意组合可以是可不受限访问的。或者，访问信息可以指定具体媒体内容仅可播放有限次。主机设备 102 可以被终端用户使用来向服务提供者 106 传送购买信息。主机设备 102 可以接收更新的访问信息，其可以被提供给存储器设备 106 以允许对安全文件 132 的访问。这种访问可以没有进一步限制、或有更宽松的限制，诸如可以浏览媒体内容更多次。

在另一具体示例实施例中，服务提供者可以使用诸如存储器设备 110 的具有安全特征(feature) 诸如控制结构 128 的非易失性可重写存储器设备，以控制包括安全文件 132 的媒体内容的分发。因此，作为媒体分发的另一方法，可以给存储器设备 110 配备安全特征，这使得服务提供者 106 能够在存储器设备 110 上创建其自身的安全环境。服务提供者 106 可以创建可以由控制器 120 执行以控制要如何使用在存储器设备 110 中存储的媒体内容的控制结构 128。控制结构 128 可以采用层次树的形式，该层次树的形式可以被服务提供者 106 配置以确定如何在存储器设备 110 处使用和访问媒体内容。控制结构 128 还可以采取称作权限对象的对象的形式。权限对象可以包括与具体媒体内容和（多个）确定验证需求相关联的访问权限和/或访问规则。在具体示例实施例中，当满足这种验证需求时，对具体媒体内容的访问得到准许并根据

访问权限和/或规则来控制。通过使用控制结构 128，多个应用可以能够访问相同内容，而不共享密钥或证书。另外，控制结构 128 可以允许控制器来把访问权限委托(delegate)给用于解密和/或加密内容的特定密钥。

图 2 是用于管理对存储在存储器中的加密文件的安全访问的系统 200 的第二具体示例实施例。系统 200 包括存储器系统或设备 202，该存储器系统或设备 202 可以经由主机接口总线 206 与主机设备 204 通信，且可以经由快闪接口总线 240 与闪存 208 通信。在具体示例实施例中，在虚线框中的存储器设备 202 和闪存 208 的所有组件（总体由标记数字 210 表示）可以被包覆在单个外壳或单元中，诸如在存储卡、存储器芯片、拇指驱动器、另一存储器设备或其任意组合中。在替换的实施例中，闪存 208 可以可移除地耦合于存储器设备 202。存储器设备 202 包括中央处理单元 (CPU) 212。存储器设备 202 还包括外围访问模块 (peripheral access module, PAM) 214、主机接口模块 (host interface module, HIM) 216、缓冲器管理单元 (buffer management unit, BMU) 218、和快闪接口模块 (flash interface module, FIM) 220。PAM 214 将 HIM 216、BMU 218、和 FIM 220 耦合于 CPU 212。

存储器设备 202 经由 HIM 216 且经由主机接口总线 206 与主机设备 204 通信。HIM 216 适用于与主机设备 204 通信，该主机设备 204 可以是数字摄像机、个人计算机、个人数字助理 (PDA)、数字媒体播放器、便携式媒体设备（诸如运动图像专家组层 3 (MP3) 播放器）、移动通信设备（诸如移动电话）、其他电子设备、或其任意组合。

可以是 NAND-型闪存的闪存 208 可以被用于为主机设备 204 提供数据存储。闪存 208 可以是可由 CPU 212 访问，且可以由 CPU 212 执行的软件代码可以被存储在闪存 208 中。CPU 212 可以包括一个或多个 CPU 随机访问存储器 (CPU RAM) 238。闪存 208 可以是经由 HIM 216、PAM 214 和 FIM 218 可被主机设备 204 访问。FIM 218 经由快闪接口总线 240 与闪存 208 通信。

BMU 218 包括与 HIM 216 通信的主机直接存储器访问 (DMA) 224。主机 DMA 224 允许 BMU 214 独立于 CPU 212 而从 HIM 216 读取和/或向 HIM 216 写数据。DMA 224 允许 BMU 218 经由 HIM 216 向主机设备 204 和从主机设备 204 传输数据，而不招致在 CPU 212 处的相关负荷 (overhead)。BMU 218 还包括寄存器 226、快闪直接存储器访问 (DMA) 228、仲裁器 232、缓冲器随机访问存储器 (BRAM) 234、和加密 (crypto) 引擎 222（加密-引擎

222)。仲裁器 232 可以是共享的总线仲裁器，以便在任何时刻仅一个主导器 (master) 或起动器 (这可以是主机 DMA 224、快闪 DMA 228 或 CPU 212) 允许活跃以与作为 BRAM 234 的从装置 (slave) 或目标装置 (target) 通信。仲裁器 232 将适当的起动器请求引导 (channel) 到 BRAM 234。主机 DMA 224 和快闪 DMA 228 负责在 HIM 216、FIM 220、BRAM 234、CPU 随机访问存储器 (CPU RAM) 238 或其任意组合之间传输的数据。

BMU 218 还包括向 CPU 212 的 CPU RAM 238 直接传送信息的 BMU 到 CPU 接口 236。BMU 218 还包括加密密钥生成器 230，加密密钥生成器 230 由加密-引擎 222 用来创建加密密钥并使用加密密钥来加密文件数据以便生成安全文件。

闪存 208 可以包括安全存储器区域 242，该安全存储器区域 242 包括加密密钥标识符 (ID)。闪存 208 还可以包括公共存储器区域 244，该公共存储器区域 244 包括具有头 248 和内容 250 的安全文件 246。头 248 可以包括元数据和与相关联于内容 250 的尾部数据相关的位置信息。可以由存储器设备 202 管理对安全文件 246 的访问和对安全区域 242 的访问。

BRAM 234 被用于存储在主机设备 204 和闪存 208 之间传递的数据。为了提高闪存 208 中存储的内容的安全性，存储器设备 202 生成用于加密和/或解密的 (多个) 密钥值。但是，通常逐个文件地进行加密和解密，这是因为主机设备 204 以文件的形式向存储器设备 202 读和写数据。类似于许多其他类型的存储设备，存储器设备 202 不一定知道文件或文件系统。虽然闪存 208 确实存储了文件分配表 (FAT) (其中标识了文件的逻辑地址)，但是通常由主机设备 204，而不由 CPU 212 访问和管理 FAT。因此，为了加密某具体文件中的数据，CPU 212 可能依赖于主机设备 204 来发送与该文件相关联的数据在存储器 208 的逻辑地址，以便可以找到该具体文件的数据，以及存储器设备 202 可以使用仅可用于存储器设备 202 的 (多个) 密钥值来对其加密和/或解密。

为了为主机设备 204 和存储器设备 202 两者均提供参考用于加密地处理这种数据的 (多个) 相同密钥的处理手段 (handle)，主机设备 204 提供对于由存储器设备 202 生成的每个密钥值的引用，其中这种引用可以是加密密钥 ID。存储器设备 202 可以访问闪存 208 的安全区域 242 来基于密钥 ID 确定相关联的加密密钥。

通常，主机设备 204 将由存储器设备 202 加密地处理的每个文件与加密密钥 ID 和存储器地址相关联。存储器设备 202 将用于加密地处理数据的每个密钥值与由主机设备 204 提供的加密密钥 ID 相关联。当主机设备 204 请求加密地处理文件时，主机设备 204 向存储器设备 202 发送请求，该请求包括加密密钥 ID 和要从存储器设备 208 取出或要被存储在存储器设备 208 处的数据的逻辑地址。存储器设备 202 生成密钥值，且将由主机 204 提供的加密密钥 ID 与所生成的密钥值相关。存储器设备 202 加密地处理从存储器设备 208 取出或要在存储器设备 208 处存储的数据。因此，存储器设备 202 可以控制（多个）加密密钥的生成和管理，且可以控制相关联的加密处理，同时允许主机设备 204 控制文件地址表（FAT）。

虽然存储器设备 202 被示出为包括存储卡形式的闪存 208，但是在此公开的系统和方法还可以应用于其他类型的存储介质，包括磁性存储介质、光存储介质、或其他类型的可重写非易失性存储介质。另外，在此公开的系统和方法还可以应用于访问这种存储介质的各种设备，包括计算设备、便携式媒体播放器、便携式通信设备、个人数字助理（PDA）、游戏系统、其他电子设备、或其任意组合。

由主机设备 204 提供的加密密钥 ID 和由存储器设备 202 生成的密钥值可以形成称作“内容加密密钥”或 CEC 的量的两个属性。在具体示例实施例中，主机设备 204 可以将每个加密密钥 ID 和与闪存 208 相关联的文件地址表中的一个或多个文件和/或一个或多个文件地址相关。在实施例中，主机设备 204 还可以将每个加密密钥 ID 与未组织的数据、非结构化的数据、结构数据、以任何形式组织的数据、或其任意组合相关。因此，加密密钥 ID 可以与未必组织到文件结构中的数据相关。

为了用户或应用获得对存储器 208 的受保护的内容或安全存储器区域的访问，存储器设备 202 可以使用可以用证书来验证用户或应用，该证书可以向存储器设备 202 预注册或在存储器 208 的安全区域中预装载。证书可以包括对称密钥、数字签名、数字证书、其他提供验证的指示物、或其任意组合。在具体示例实施例中，证书可以与被授权给具体用户、具体设备或具体应用的访问权限相关联。在具体实施例中，证书可以是访问码、密码、序列号、其他数据，或其任意组合。在预注册处理中，存储器设备 202 存储用户、设备和应用的标识和证书的记录。存储器设备 202 还可以存储与由用户或应用

确定的、且经由主机设备 204 提供的这种标识和证书相关联的访问权限。在已经完成了预注册之后，当用户或应用请求将数据写到存储器 208 时，用户或应用提供与其标识和证书相关的数据、用于加密数据的加密密钥 ID、和该加密数据要存储于存储器 208 的逻辑地址。存储器设备 202 生成密钥值，并将该值与由主机设备 204 提供的加密密钥 ID 相关联，且在它的用于该用户或应用的记录或表格中存储针对加密数据的密钥值的加密密钥 ID。然后，存储器设备 208 加密该数据，且在由主机设备 204 指定的地址处存储加密数据。存储器设备 202 还在数据文件的头部分中存储加密密钥 ID。存储器设备 202 还可以在存储器 208 的安全部分中存储加密密钥 ID 数据。

图 3 图示了其中具有安全特征的存储器设备、诸如在图 2 中的存储器设备 210 可以用于安全地存储媒体内容且用于以受控方式递送其中存储的媒体内容的环境。如图 3 所示，系统 300 包括内容提供者 310，该内容提供者 310 可以包括可以经由网络、诸如因特网、无线网络、公共交换电话网络、分组交换网络、其他网络或其任意组合与远程设备通信的一个或多个服务器。内容提供者 310 可以包括内容服务器 312 和存储卡管理服务器 314。内容服务器 312 可以包括音乐数据、视频数据、多媒体内容、或其任意组合。另外，内容服务器 312 可以提供用于标识媒体内容、用于确定与递送和回放所标识的媒体内容相关的访问供应和设备偏好、用于经由适当的通信路径递送媒体内容的搜索功能、供应 (provisioning) 功能、和递送功能。例如，来自媒体内容服务器 312 的媒体内容可以经由诸如基站 304 的基站提供给移动网络 324，该移动网络 324 与一个或多个移动设备 302 通信。此外，内容服务器 312 可以经由可以是诸如因特网的广域网的网络 320 与其他设备、个人计算设备 306、个人数字助理 (PDA) 308、便携式媒体播放器 316 (诸如 MP3 播放器)、游戏系统 318、其他设备、或其任意组合通信。

内容提供者 310 可以提供媒体内容，可以把媒体内容存储在存储设备 322 中，存储设备 322 包括具有 (多个) 加密密钥标识符 (ID) 324 的安全存储器区域且包括公共存储器区域 326。公共存储器区域 326 可以包括安全文件 328，其包括头部 330 且具有内容部分 332，该头部 330 具有元数据和与尾部数据相关的位置信息。可以由各种不同终端用户端或主机、包括 PDA 308、视频游戏系统 318、移动电话 302、MP3 播放器 316、和可以包括桌面型计算机、便携式计算机或其任意组合的计算机 306 来呈现(render)从内容提

供者 310 递送的媒体内容。与每个用户端或主机相关联的存储器设备可以包括可以由设备提供者配置以提供对于媒体内容分发的途径（avenue）的安全存储区域。

通常，可以限制对在内容服务器 312 存储的媒体内容的访问。卡管理服务器 314 可以向用户端或主机提供访问权限和/或访问规则。管理对在卡管理服务器 314 中的加密媒体内容的访问的访问权限和/或访问规则可以当媒体内容由手机 302、由其他类型的终端诸如媒体播放器 316 和计算机 306 访问时应用。也可以由服务提供者、诸如无线网络运营者把内容和权限和/或规则提供给计算机 306 或给移动电话设备 302。

在图 3 的环境中，可使用用于存储和分发媒体内容的存储器系统的多种途径。在一种方法中，闪存卡制造者卖存储卡给内容发布者，该内容发布者还从内容提供者购买媒体内容并从权限对象服务器接收用于控制这种内容的（多个）权限对象。在这种内容和（多个）权限对象被装载到卡之前，内容发布者首先经由与验证服务器的连接来确认该卡是否是真实的。在验证了该卡之后，该内容和（多个）权限对象被装载。可以在内容提供者 310 处提供验证服务器。

因此，内容发布者（其还可以是卡制造者）卖卡给诸如移动网络运营者的服务提供者。然后，服务提供者把卡连同终端用户终端诸如由原始器件制造者（Original Equipment Manufacturer，称为“OEM”）提供的蜂窝电话机一起销售。在内容发布者卖卡给服务提供者之前，内容发布者可以安装在此描述的类型的控制结构。优选地，由所描的服务提供者来安装这种控制结构以使得服务提供者能够创建其自己的安全环境，以便其可以控制内容分发。在此之前，卡被再次确认是真实的。因此，在服务提供者的机构处，通过连接到验证服务器来再次验证该卡。还经由终端来将卡连接到验证服务器来使能或激活在卡中的任何具体部件或应用（例如，诸如媒体播放器的媒体内容呈现应用）。然后，服务提供者安装控制结构以控制对卡中内容的访问。控制结构规定了仅授权的用户可以能够访问内容，且这种访问将符合在控制结构中的特定许可或符合特定权限和/或规则。

或者，内容发布者可以直接卖卡给终端用户。该终端用户从 OEM 获得诸如蜂窝电话机的终端。在这种终端和卡可以相互验证的情况下，则终端用户将能够使用该终端来访问存储在存储卡中的内容。在该配置中，给该终端

用户提供验证信息，诸如用于访问内容的证书（用户标识符、密码、序列号等）。该验证处理防止了没有被提供有适当的验证的其他人以未授权的方式访问该内容。

或者，在预览内容被内容发布者装载到卡中的情况下，这种内容还可以包括媒体内容的加密未删节版本。因此，当终端用户购买这种卡时，该卡将已经存储了用户想要购买的媒体内容的加密版本。该卡还应已存储了限制终端用户权限以仅访问卡中内容的删节版本或部分的权限和/或规则。在这种情况下，不需要再次将这种内容下载到卡中。而是，终端用户将需要的全部就是用于解密媒体内容的内容加密密钥和更新管理这种访问以允许不受限或更宽松的访问的权限和/或规则。这种信息可以在验证之后通过服务提供者从权限发布者下载。

在另一实施例中，仅在终端用户订阅了服务诸如由服务提供者提供的服务之后才可以由终端用户访问在卡中的内容。因此，由终端用户购买的卡将包含控制信息，该控制信息不允许终端用户访问内容直到终端用户已经订阅。终端用户可以首先从内容发布者购买该卡，但将不能够访问其中的媒体内容，直到他或她从服务提供者购买了订阅。在确认订阅之前，终端用户所持有的卡被验证服务器查证为真实的，且由验证服务器可选地使能或激活应用（例如，诸如媒体播放器的媒体内容呈现应用）。在订阅处理中，权限发布者所提供的权限对象由服务提供者传输到终端用户以供下载到卡。

在替换的方法中，由终端用户购买的卡将不具有预装载的媒体内容。终端用户将必须从服务提供者购买内容，而服务提供者继而从内容提供服务器获得内容。如之前所述的，在将内容装载到卡之前，由验证服务器来验证该卡。由验证服务器可选地使能特征和应用（例如，诸如媒体播放器的媒体内容呈现应用）。作为交易的一部分，通过服务提供者将来源于权限发布者的权限对象传输到终端用户以供下载到卡。虽然由终端用户购买的卡可以不具有预装载的媒体内容，但是该卡中可以存储了（多个）权限对象，该（多个）权限对象授权终端用户来下载这种内容。则这是一种预付费的媒体内容卡，其使得终端用户能够重复下载所购买的内容。

参考图 4，图示了在非易失性存储器中存储内容的方法的具体实施例。在 402，该方法包括读取包括媒体内容和包括尾部的内容文件。该尾部包括与媒体内容相关的尾部数据，且可以包括诸如 ID3 数据的元数据。该方法还

包括：在 404，在文件诸如安全文件的头部分中存储与尾部数据相关的位置信息以及安全数据，且如 406 所示，将文件存储到非易失性存储器或耦合于非易失性存储器设备的主机设备的存储器区域的存储元件。主机设备可以是包括处理器和存储器的电子设备，诸如电话设备、个人数字助理（PDA）、膝上型计算机或桌面型计算机。在具体实施例中，结合在文件的头部分中存储尾部数据与安全数据而使用应用编程接口（API）。在存储了该文件之后，可以从存储器提取内容，且可以向主机设备提供媒体内容用于回放，如 408 所示。回放可以包括音频内容的音频回放、视频内容的视频回放或多媒體內容的多媒體回放。

在具体示例实施例中，内容提供者可以要求保护被存储在非易失性存储器中的内容。在该情况下，可以使用安全会话来访问受保护的内容。例如，可以在非易失性存储设备和主机设备之间建立安全会话。非易失性存储设备可以使用内容加密密钥来解密该内容。然后，可以使用与安全会话有关的会话密钥来加密被解密的内容。可以使用安全会话向主机设备提供加密的数据。然后，主机设备可以使用会话密钥来解密该内容。通过利用安全会话程序，可以当由主机设备回放时保护该内容。

参考图 5，示出了提取内容的方法的具体实施例。该方法包括在 502、从非易失性存储器读取内容，以及在 504 从安全文件的头部分读取关于与该内容相关联的尾部数据的位置信息。该头部分包括与该内容相关的安全数据项。该方法还包括在 506、向具有对非易失性存储器的访问的主机设备的显示设备提供与该尾部数据相关的数据。在具体实施例中，主机设备访问以读取该内容用于诸如通过使用回放程序（例如，媒体播放器）回放。该内容可以包括音频数据、视频数据、或多媒体数据。在具体实施例中，结合从安全文件的头部分读取尾部数据而使用应用编程接口（API）。主机设备可以将文件名和元数据结构传递给文件系统工具包，其中该文件系统工具包使用 API 来将元数据写到安全文件的头部分。可以在主机设备处回放该内容，如 508 所示。另外，可以使用从该头提取的元数据来在主机设备上的显示设备上显示关于该内容的信息，诸如在主机设备上显示内容标题、艺术家名、或其他内容相关信息。显示设备可以是在蜂窝电话或 MP3 播放器上的显示器或耦合于计算机的显示设备。如上所述，可以使用安全会话来保护在主机设备回放的内容，从而允许非易失性存储器设备向该主机设备提供安全的内容，而不将加密密

钥暴露于该主机设备。

参考图 6，示出了使用非易失性可重写存储器来访问媒体内容的方法。该方法包括在 602 接收关于访问权限的信息，并在非易失性可重写存储器的安全存储器区域中存储访问权限。在 604，这些访问权限允许访问内容解密密钥，该内容解密密钥用于解密在非易失性可重写存储器中存储的加密媒体内容。该方法还包括在 606 供应至少一个所选的加密媒体内容项的解密版本，且在 608 供应从安全存储器区域的头部分提取的元数据。该元数据与该至少一个所选的加密媒体内容项相关联。可以将该至少一个所选的加密媒体内容的解密版本提供给主机设备。主机设备可以是电话设备、个人数字助理 (PDA)、计算机或其他类型的设备。

该方法还可以包括在 610 接收验证信息，并在接收验证信息之后使用内容解密密钥解密该至少一个所选的加密媒体内容项。主机设备可以包括回放设备，其用于呈现该至少一个所选的加密媒体内容项的解密版本。在具体实施例中，该方法还包括在 612 将主机设备连接到服务器，在 614 从主机设备发送购买授权给服务器，以及在 616 在主机设备处接收访问权限，并在 618 向非易失性可重写存储器供应验证信息和访问权限以允许对所选的加密媒体内容项的访问。

可以显示关于从该头提取的元数据的信息，如 620 所示，且可以在 622 当主机同时显示关于元数据的信息的同时呈现该至少一个所选的加密媒体内容项的解密版本。例如，可以在主机设备上回放歌曲的音频文件的同时显示歌曲标题或艺术家名。

参考图 7，图示了用于安全文件 700 的数据结构的具体例子。该安全文件 700 可以被存储在诸如计算机存储器设备的计算机只读介质上。该安全文件 700 包括头部分 702 和内容部分 710。内容部分 710 包括一个或多个媒体内容项和尾部数据 712。该头部分 702 包括安全数据段 704、元数据段 706、和尾部数据位置 708。安全数据段 704 可以包括加密密钥标识符 (ID)、隐藏数据、或其他数据保护信息。

参考图 8，示出了文件的头部分的代表性数据结构。该头部分 800 包括长度字段 802、类型字段 804、签名字段 806、版本字段 808 和填充 (padding) 810。在具体实施例中，该头数据结构可以包括可变数量个字段 (也称为框)。字段或框的每个包括可变数量的字节的数据，其中每个框前面具有四字节的

长度。

参考图 9，示出了可以被存储在头中的元数据的代表性数据结构。元数据 900 包括长度字段 902、类型字段 903、内容名长度字段 904、内容名填充字段 906、艺术家名长度字段 908、艺术家名填充字段 910、专辑名长度字段 912、专辑名填充字段 914、流派订阅者长度字段 916、流派订阅者填充字段 918、其他项的长度字段 902、和其他项的其他子框 922。在具体例子中，该类型字段 903 可以包括指定符“mdat”来标识元数据。而且，在具体示例实施例中，内容名的长度 904、艺术家名的长度 908、和专辑名 912 的长度每个可以是 64 字节。通过使用在头部分中的元数据数据结构，诸如音频或视频文件的相关内容文件的元数据可以供在回放内容文件期间快速访问和随后显示的方式方便地存储。该方法提供对用于已经被存储在诸如非易失性存储器设备的存储器中的加密内容文件的元数据的有效地存储和提取。

参考图 10，示出了可以被存储在文件的头部分中的尾部数据的数据结构 1000。该尾部数据结构 1000 包括长度字段 1002、类型字段 1004、标记 1006、扇区数量字段 1009、记录日期/时间字段 1010、文件的第一扇区的簇号字段 1012、尾部的簇号字段 1014、尾部的下一簇（如果存在）字段 1016、扇区偏移量字段 1018、和字节偏移量字段 1020。在具体示例实施例中，尾部信息的框长度是 4 字节，且该框类型字段 1004 被填入了指示符“Idat”来指定尾部数据。该标记字段 1006 可以包括指示该尾部是否与扇区边界对齐的第一比特和指示该尾部是否包含不止一个扇区的第二比特，直到在簇中的最大数量的扇区。该记录日期/时间 1010 被用于来检查该文件是否已经被移动，或是具有尾部框的文件的副本。如果用户已经完成了在个人计算机上的移动或复制，则将进行传统的文件搜查操作。如果该尾部数据跨越了两个不同的簇，则下一簇字段 1016 被用于标识下一簇。两个簇可以不连续。

尾部数据结构提供包括该文件的尾部数据的具体簇、扇区和字节位置信息的信息。通过在该文件的头部分中存储尾部数据位置信息，主机设备可以根据该头快速且有效地访问尾部数据，而不需要文件系统进行多个加密文件的大且长的搜索来提取具体尾部数据。因此，该公开的方法和系统提供更快更有效的访问来提取加密内容文件的尾部数据。

在此描述的实施例的图示意图提供各种实施例的结构总体理解。这些图示不意图用作使用在此描述的结构或方法的装置和系统的所有元件和部件的

完整描述。对于浏览了该公开的本领域技术人员可以清楚许多其他实施例。可以使用和从该公开中导出其他实施例，因此可以进行结构和逻辑上的替换和改变，而不偏离该公开的范围。另外，这些图示仅是代表性的，且可能未按比例画图。可以扩张在图示中的特定比例，同时可以减少其他比例。虽然已经图示和描述了具体实施例，但应该理解，设计来实现相同或类似目的的任何随后的布置都可以替换所示的具体实施例。该公开意图覆盖各种实施例的任意和所有随后的适应或变体。在浏览了该说明书之后，本领域技术人员将清楚上述实施例、在此未具体描述的其他实施例的组合。因此，该公开和图应视为例示而非限制。

基于如下理解提交该公开的摘要：该公开的摘要不用来解释或限制权利要求的范围或含义。另外，在之前具体描述中，为了本公开连贯的目的，在单个实施例中可能把各种特征分组到一起或来描述。该公开不应被解释为反映所声明的实施例需要比在每个权利要求中明确陈述的特征更多的特征的意图。而是，如以下权利要求反映的，因此本发明的主题可以定为比任一所公开实施例的所有特征少。因此，随后的权利要求被并入具体实施例描述中，其中，每个权利要求独立自主地定义了要求的主题。

上述公开的主题应视为例示性，而不是限制性，且所附权利要求意图覆盖所有这种修改、增强和其他实施例，这些均落入本发明的真实精神和范围。因此，至法律允许的最大延展度，本发明的范围要由随后权利要求和其等同物的最宽可允许的解释来确定，而不应该由先前的详细描述来限制或局限。

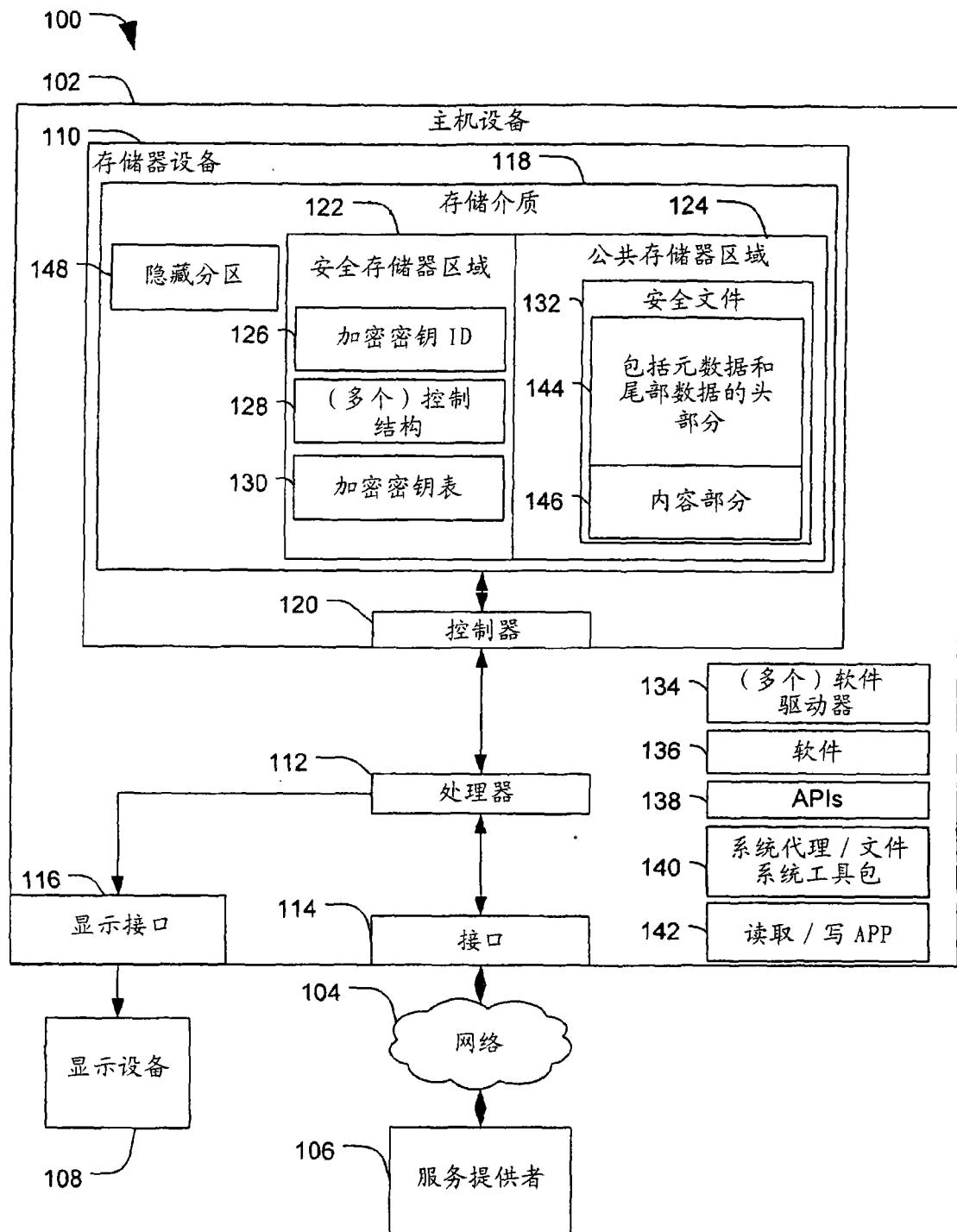


图 1

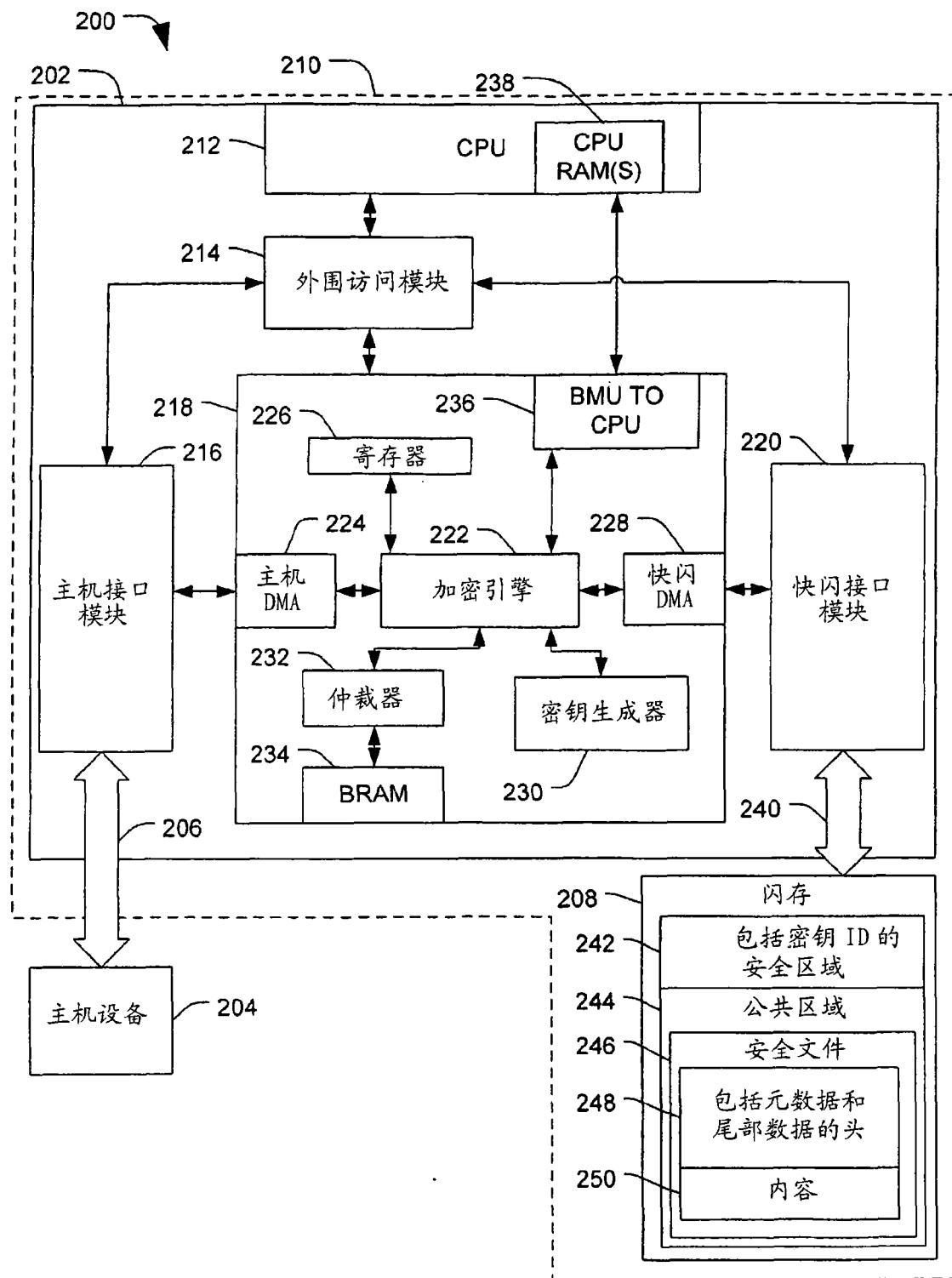


图 2

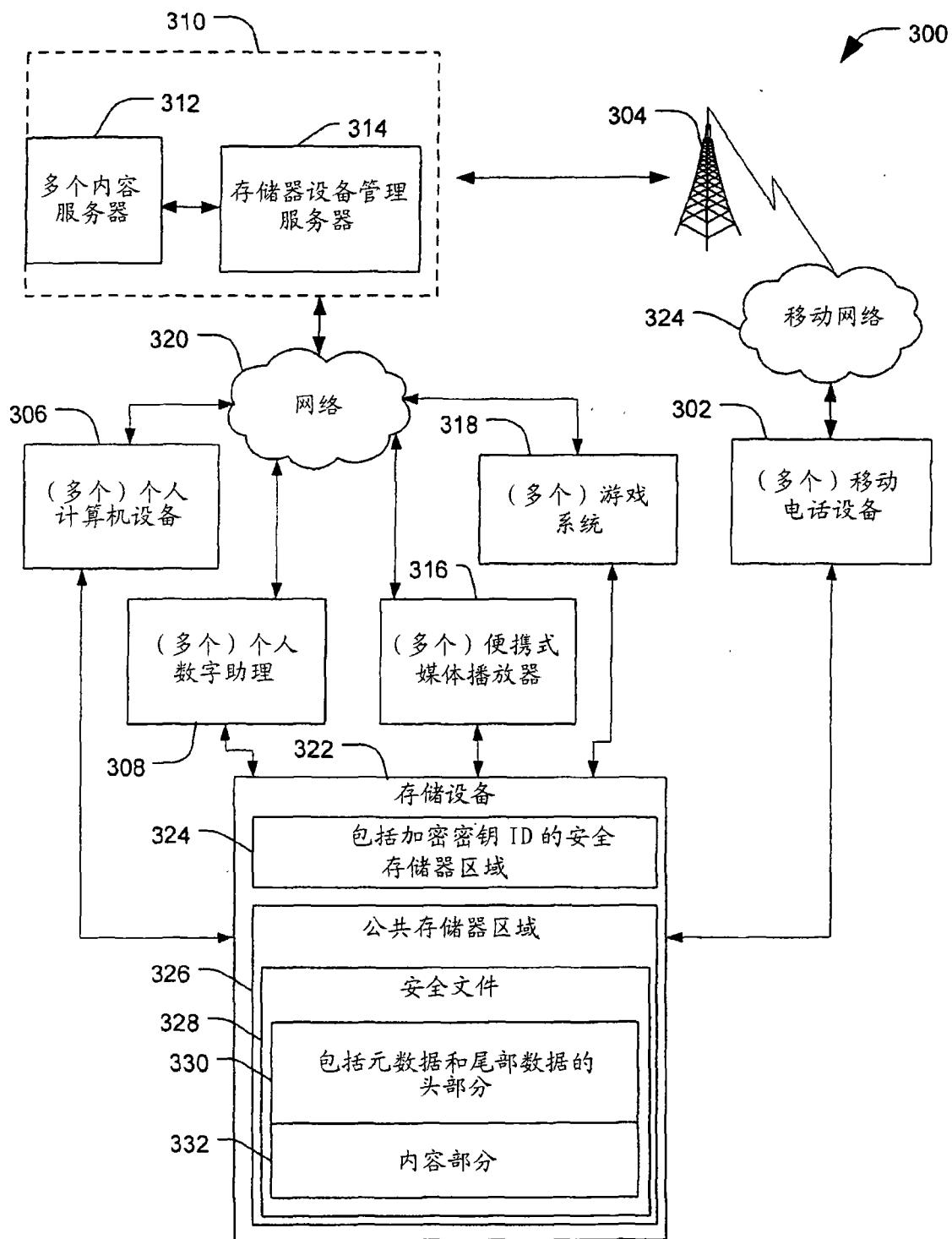


图 3

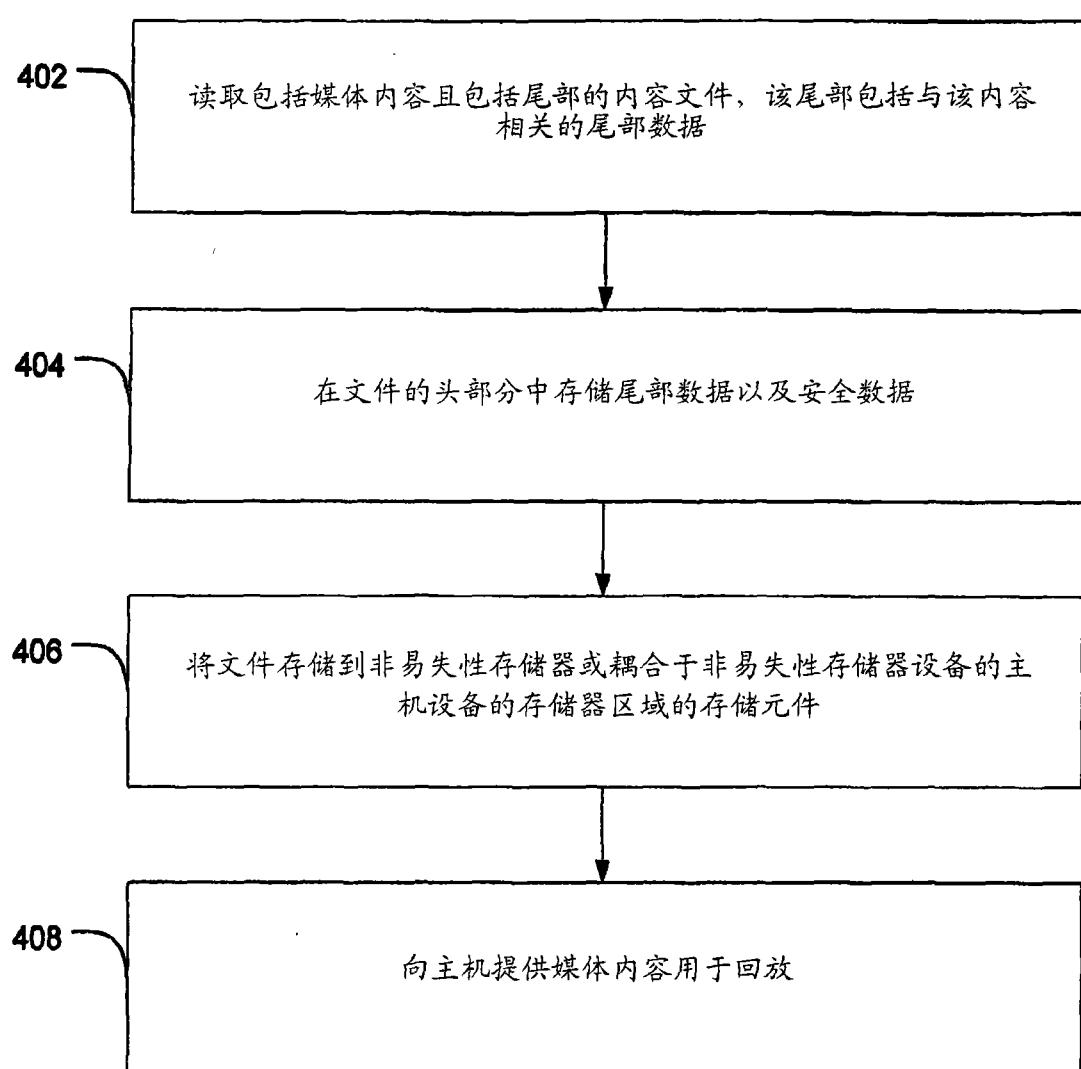


图 4

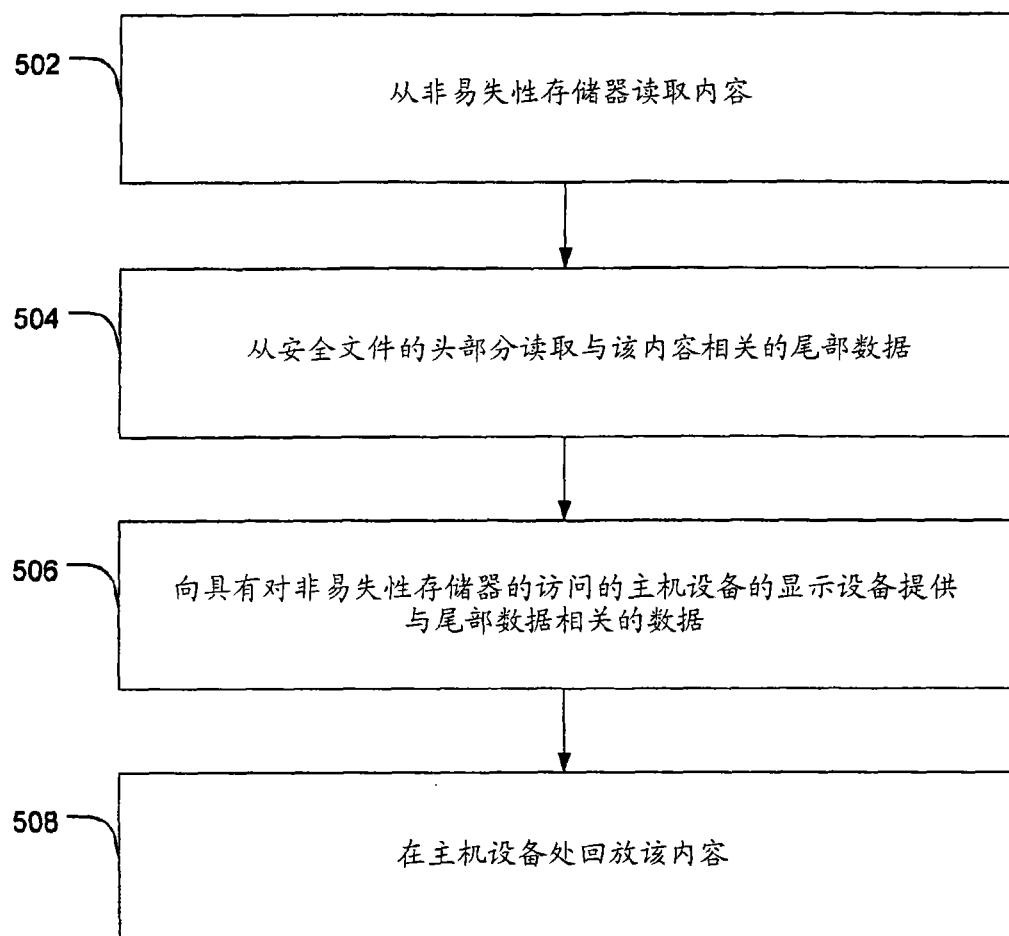


图 5

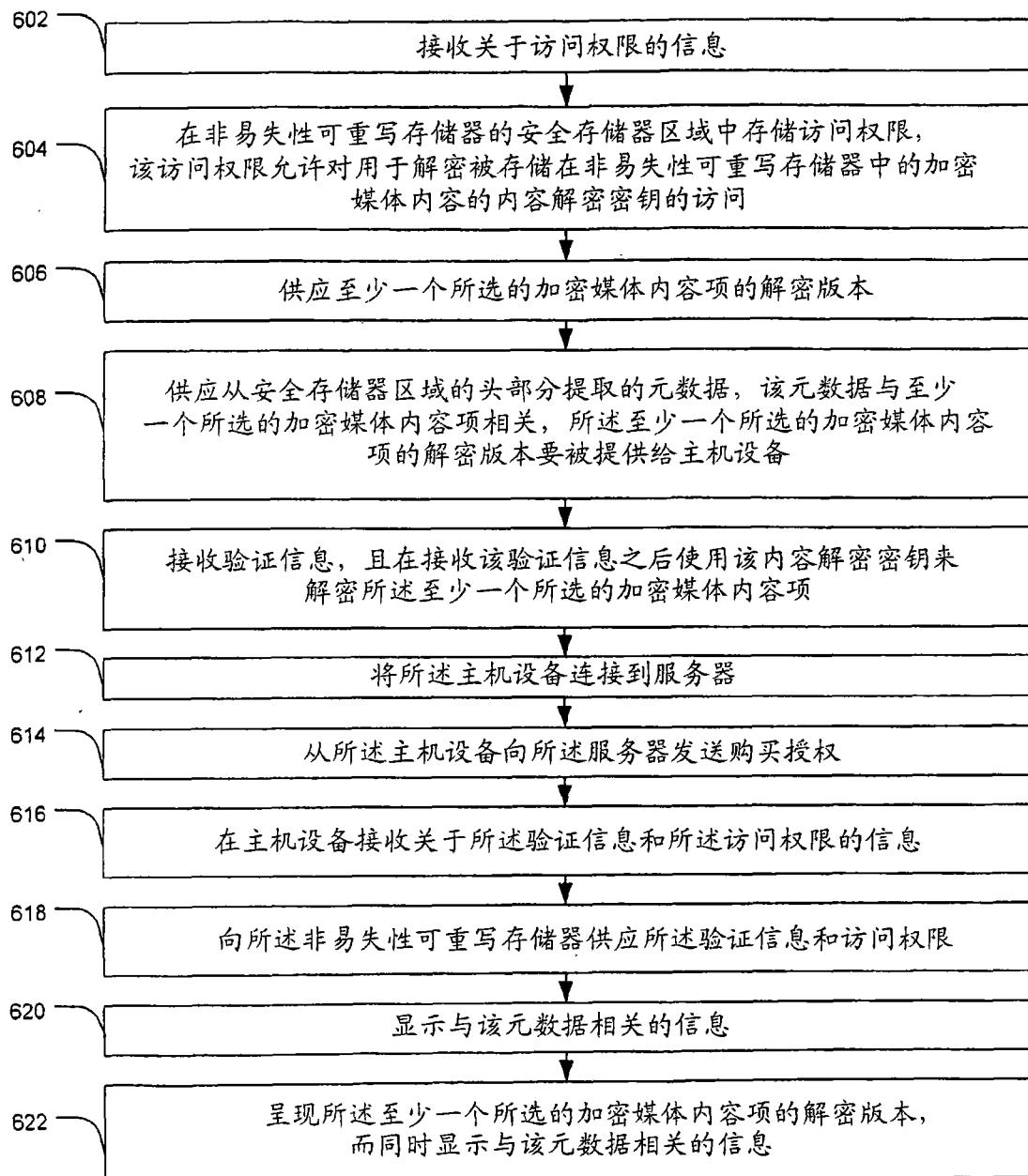


图 6

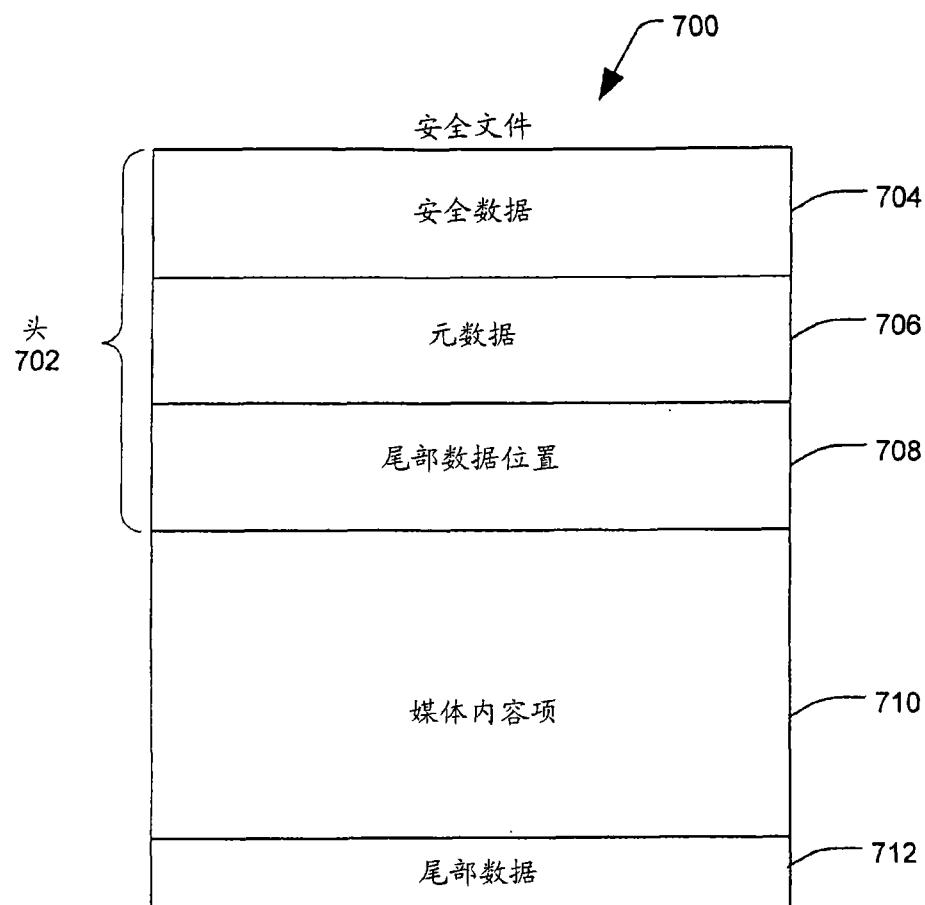


图 7

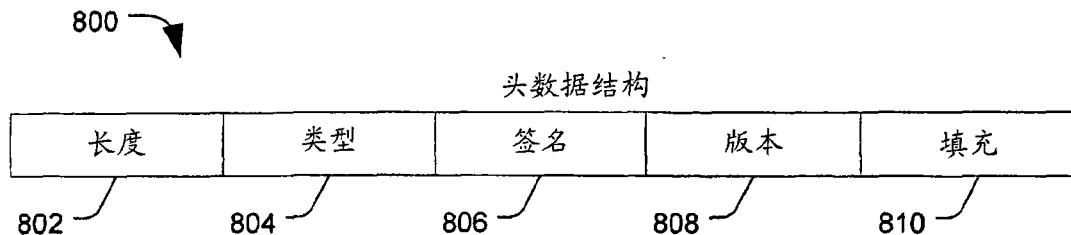


图 8

元数据结构

长度 <u>902</u>	类型 <u>903</u>	内容名长度 <u>904</u>	内容名填充 <u>906</u>	
艺术家名长度 <u>908</u>		艺术家名填充 <u>910</u>	专辑名长度 <u>912</u>	专辑名填充 <u>914</u>
流派子集长度 <u>916</u>	流派子集填充 <u>918</u>	长度 <u>920</u>	其他子集填充 <u>922</u>	

图 9

尾部数据结构

长度 <u>1002</u>	类型 <u>1004</u>	标记 <u>1006</u>	扇区数 <u>1008</u>	呈现日期 / 时间 <u>1010</u>
该文件的第一扇区 的簇号 <u>1012</u>	尾部的簇号 <u>1014</u>	尾部的下一簇 (如果存在) <u>1016</u>	扇区 偏移量 <u>1018</u>	字节 偏移量 <u>1020</u>

图 10