(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101739518 B
(45)授权公告日 2012.07.18

(21)申请号 200810178635.5
(22)申请日 2008.11.21
(73)专利权人 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 周继扬 周佩燕 林育中
(74)专利代理机构 北京市柳沈律师事务所 11105
代理人 蒲迈文
(51)Int.Cl.
G06F 21/00(2006.01)
H04L 29/06(2006.01)

(56)对比文件
JP 2005535958 A,2005.11.24, 全文.
CN 1777851 A,2006.05.24, 全文.
US 20050228995 A1,2005.10.13, 全文.

审查员 马毓昭

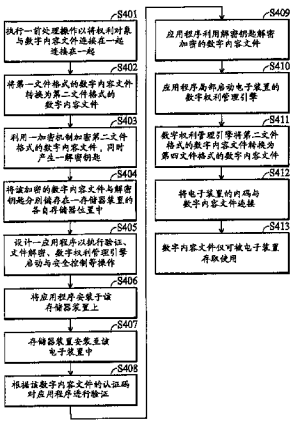
权利要求书 3 页 说明书 7 页 附图 7 页

(54)发明名称

局部启动数字权利管理引擎的方法与系统

(57)摘要

一种局部启动数字权利管理引擎的方法。将权利对象连接至第一文件格式的数字内容文件，并且转换为第二文件格式的数字内容文件。加密该第二文件格式的数字内容文件并且产生对应解密钥匙。将该应用程序安装在该存储器装置中，并且安装该存储器装置至电子装置中。根据该数字内容文件的认证码对该应用程序进行验证，并且通过该应用程序并利用该解密钥匙解密该加密的数字内容文件，并且启动该电子装置的数字权利管理引擎。通过该数字权利管理引擎将该电子装置的内码与该数字内容文件及权利对象连接，使得该数字内容文件仅可被该电子装置存取使用。



CN 101739518 B

1. 一种局部启动数字权利管理引擎的方法，其应用于电子装置，包括下列步骤：

执行前处理操作，其将权利对象与第一文件格式的数字内容文件连接在一起；

将该第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件；

加密该第二文件格式的数字内容文件以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙；

将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中；

设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序；

将该应用程序安装在该存储器装置；

安装该存储器装置至该电子装置中；

根据该数字内容文件的认证码对该应用程序进行验证；

当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件；

通过该应用程序局部启动该电子装置的数字权利管理引擎；以及

通过该数字权利管理引擎将该第二文件格式的该数字内容文件转换为第四文件格式的数字内容文件，然后将该电子装置的内码与该第四文件格式的该数字内容文件连接，使得该第四文件格式的该数字内容文件仅可被该电子装置存取使用。

2. 根据权利要求 1 所述的局部启动数字权利管理引擎的方法，其中，加密该数字内容文件的步骤还包括将该第二文件格式的数字内容文件转换为该第三文件格式的数字内容文件。

3. 根据权利要求 1 所述的局部启动数字权利管理引擎的方法，其中，替代上述将该解密钥匙储存在存储器装置的各自存储区域中而将该解密钥匙分散储存于该存储器装置。

4. 根据权利要求 1 所述的局部启动数字权利管理引擎的方法，其中，该认证码可为该数字内容文件的专属序号或该存储器装置的唯一序号。

5. 一种局部启动数字权利管理引擎的系统，包括：

执行前处理操作，其将权利对象与第一文件格式的数字内容文件连接在一起的装置；

将该第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件的装置；

加密该第二文件格式的数字内容文件以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙的装置；

将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中的装置；

设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序的装置；

将该应用程序安装在该存储器装置的装置；

安装该存储器装置至该电子装置中的装置；

根据该数字内容文件的认证码对该应用程序进行验证的装置；

当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自第三

文件格式的数字内容文件还原至该第二文件格式的数字内容文件的装置；

通过该应用程序局部启动该电子装置的数字权利管理引擎的装置；以及

通过该数字权利管理引擎将该第二文件格式的该数字内容文件转换为第四文件格式的数字内容文件，然后将该电子装置的内码与该第四文件格式的该数字内容文件连接，使得该第四文件格式的该数字内容文件仅可被该电子装置存取使用的装置。

6. 根据权利要求 5 所述的局部启动数字权利管理引擎的系统，其中，该解密钥匙是分散储存于该存储器装置。

7. 一种局部启动数字权利管理引擎的方法，其应用于电子装置，包括下列步骤：

执行前处理操作，将第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件，其中权利对象与第一文件格式的数字内容文件是分开储存；

加密该第二文件格式的数字内容文件，以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙；

将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中；

设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序；

将该应用程序安装在该存储器装置；

安装该存储器装置至该电子装置中；

根据该数字内容文件的认证码对该应用程序进行验证；

当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自该第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件；

通过该应用程序局部启动该电子装置的数字权利管理引擎；以及

通过该数字权利管理引擎将该第二文件格式的数字内容文件与该数字内容的权利对象以及该电子装置的内码连接，使得该数字内容文件仅可被该电子装置存取使用。

8. 一种局部启动数字权利管理引擎的系统，包括：

执行前处理操作，将第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件的装置，其中权利对象与第一文件格式的数字内容文件是分开储存；

加密该第二文件格式的数字内容文件，以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙的装置；

将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中的装置；

设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序的装置；

将该应用程序安装在该存储器装置的装置；

安装该存储器装置至该电子装置中的装置；

根据该数字内容文件的认证码对该应用程序进行验证的装置；

当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自该第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件的装置；

通过该应用程序局部启动该电子装置的数字权利管理引擎的装置；以及

通过该数字权利管理引擎将该第二文件格式的数字内容文件与该数字内容的权利对象以及该电子装置的内码连接，使得该数字内容文件仅可被该电子装置存取使用的装置。

局部启动数字权利管理引擎的方法与系统

技术领域

[0001] 本发明是有关于数据加密与解密，且特别有关于一种局部启动数字权利管理(Digital Rights Management，DRM)引擎的方法与系统。

背景技术

[0002] 数字内容可以经由在线(On-Line)传递或离线(Off-Line)传递。在线传递是经由如因特网下载数字内容，离线传递是经由特定储存媒体(例如，光盘、数字视频影碟(Digital Video Disk，DVD)或可携式电子装置(例如，手机)内建的闪存装置(例如，安全数字(Secure Digital，SD)存储卡或通用序列总线(Universal Serial Bus，USB))磁盘)来预录数字内容。

[0003] 离线传递可利用DVD的内容拦截系统(Content Scramble System，CSS)以及可录制媒体的内容保护(Content Protection for Recordable Media，CPRM)或者SD存储卡与DVD-RW的预录媒体的内容保护(Content Protection for Pre-Recorded Media，CPPM)来保护。

[0004] 一般数字内容的使用需经过数字权利管理系统的处理，才能确保该装载的数字内容不会被非法使用或盗版。

[0005] 图1是显示传统数字权利管理引擎处理的方法步骤流程图。

[0006] 经过预处理的数字内容文件被储存于网络上的文件服务器上(步骤S11)。当消费者取得授权后，经过预处理的数字内容文件被下载与储存在电子装置中(例如，个人计算机或移动电话)(步骤S12)，并同时启动该电子装置上的数字权利管理引擎(步骤S13)。将该预处理的数字内容文件与该电子装置所持有的内码(International Mobile Electron Identification，IMEI)以及权利对象结合(步骤S14)，以利用数字权利管理引擎将该预处理的数字内容文件转换成只能在该电子装置上使用的文件(步骤S15)。

[0007] 上述方法包括开放移动联盟(Open Mobile Alliance，OMA)的DRM处理、网络装置的Windows Media DRM 10(WMDRM-ND)处理以及Apple系统的FairPlay™处理。以OMA DRM处理为例，原始数字内容文件的文件格式为.3gp、.mp3之类的影音文件。OMA DRM会先执行预处理，以将.3gp文件转换成.dm(DRM Material)文件，然后将.dm文件储存在文件服务器上等待下载。当消费者上网购买该数字内容文件并取得权利对象(Rights Object)(即该数字内容文件)之后，该服务器上的.dm文件会被下载至消费者的电子装置上。该电子装置的数字权利管理引擎会将权利对象及其内码与数字内容连接(Bind)，并且将.dm文件转换成.dcf(DRM Content Format)文件。经此处理后，.dcf文件的数字内容文件只能在此特定电子装置依权利对象所赋予的方式使用。

[0008] 然而，上述方法的缺陷是只适用于在线传递，而且其数字权利管理方式可能违反消费者对于内容传统的使用方式及权利(Traditional Rights and Usage，TRU)。

[0009] 图2是显示另一传统数字权利管理引擎处理的方法步骤流程图。

[0010] 经预处理的数字内容文件储存于电子装置的内建存储器(Embedded Memory)中，

以加密预处理的数字内容文件（步骤 S21）。数字内容文件的权利对象可经由网络（例如，因特网）下载（步骤 S22），并且储存在该电子装置中（步骤 S23），同时启动该电子装置的数字权利管理引擎（步骤 S24）。该数字权利管理引擎先对预处理的数字内容文件解密（步骤 S25），将电子装置的内码及权利对象连接到数字内容文件（步骤 S26），并且将数字内容文件转换为新的文件格式（步骤 S27）。

[0011] 因此，该数字内容文件只能在此特定的电子装置使用。举例来说，可携式装置的 Windows Media DRM(WMDRM-PD) 的文件格式为 .asf(Advanced System Format)。上述方法适用于可携式电子装置，但权利对象需另行传送，虽然安全性稍为提高，但是仍摆脱不了对网络的依赖。

[0012] 图 3 是显示另一传统数字权利管理引擎处理的方法步骤流程图。

[0013] 不利用电子装置所支持的数字权利管理引擎，而另行设计自有的数字权利管理机制（步骤 S31）。对数字内容文件进行前处理并且转换为可被自行设计的数字权利管理引擎或系统处理的文件格式（步骤 S32）。因此，该数字内容文件仅可被包含该自行设计的数字权利管理引擎或系统的电子装置存取（步骤 S33）。上述方法面临下面几个问题 :1) 此程序撰写工程浩大 ;2) 此程序可能占用庞大存储器空间 ;3) 数字权利管理机制通常与操作系统平台的底层息息相关，动辄会有兼容性的问题 ;以及 4) 由于是自行撰写，比较缺乏业界使用经验，难获得内容业者信赖。

发明内容

[0014] 本发明的目的在于提供一种局部启动数字权利管理引擎的方法与系统。

[0015] 基于上述目的，本发明实施例揭露了一种局部启动数字权利管理引擎的方法，其应用于电子装置，包括下列步骤 :执行前处理操作，其将权利对象与第一文件格式的数字内容文件连接在一起 ;将该第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件 ;加密该第二文件格式的数字内容文件以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙 ;将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中 ;设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序 ;将该应用程序安装在该存储器装置 ;安装该存储器装置至该电子装置中 ;根据该数字内容文件的认证码对该应用程序进行验证 ;当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件 ;通过该应用程序局部启动该电子装置的数字权利管理引擎 ;以及通过该数字权利管理引擎将该第二文件格式的该数字内容文件转换为第四文件格式的数字内容文件，然后将该电子装置的内码与该第四文件格式的该数字内容文件连接，使得该第四文件格式的该数字内容文件仅可被该电子装置存取使用。

[0016] 本发明实施例还揭露了一种局部启动数字权利管理引擎的系统，包括 :执行前处理操作，其将权利对象与第一文件格式的数字内容文件连接在一起的装置 ;将该第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件的装置 ;加密该第二文件格式的数字内容文件以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙的装置 ;将该加

密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中的装置；设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序的装置；将该应用程序安装在该存储器装置的装置；安装该存储器装置至该电子装置中的装置；根据该数字内容文件的认证码对该应用程序进行验证的装置；当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件的装置；通过该应用程序局部启动该电子装置的数字权利管理引擎的装置；以及通过该数字权利管理引擎将该第二文件格式的该数字内容文件转换为第四文件格式的数字内容文件，然后将该电子装置的内码与该第四文件格式的该数字内容文件连接，使得该第四文件格式的该数字内容文件仅可被该电子装置存取使用的装置。

[0017] 本发明实施例还揭露了一种局部启动数字权利管理引擎的方法，其应用于电子装置，包括下列步骤：执行前处理操作，将第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件，其中权利对象与第一文件格式的数字内容文件是分开储存；加密该第二文件格式的数字内容文件，以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙；将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中；设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序；将该应用程序安装在该存储器装置；安装该存储器装置至该电子装置中；根据该数字内容文件的认证码对该应用程序进行验证；当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自该第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件；通过该应用程序局部启动该电子装置的数字权利管理引擎；以及通过该数字权利管理引擎将该第二文件格式的数字内容文件与该数字内容的权利对象以及该电子装置的内码连接，使得该数字内容文件仅可被该电子装置存取使用。

[0018] 本发明实施例还揭露了一种局部启动数字权利管理引擎的系统，包括：执行前处理操作，将第一文件格式的数字内容文件转换为仅可被该电子装置的一数字权利管理引擎辨识的第二文件格式的数字内容文件的装置，其中权利对象与第一文件格式的数字内容文件是分开储存；加密该第二文件格式的数字内容文件，以将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件，同时产生对应解密钥匙的装置；将该加密的数字内容文件与该解密钥匙储存在存储器装置的各自存储区域中的装置；设计用于执行验证、文件解密、数字权利管理引擎启动与安全控制的操作的应用程序的装置；将该应用程序安装在该存储器装置的装置；安装该存储器装置至该电子装置中的装置；根据该数字内容文件的认证码对该应用程序进行验证的装置；当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自该第三文件格式的数字内容文件还原至该第二文件格式的数字内容文件的装置；通过该应用程序局部启动该电子装置的数字权利管理引擎的装置；以及通过该数字权利管理引擎将该第二文件格式的数字内容文件与该数字内容的权利对象以及该电子装置的内码连接，使得该数字内容文件仅可被该电子装置存取使用的装置。

附图说明

[0019] 图 1 是显示传统数字权利管理引擎处理的方法步骤流程图。

[0020] 图 2 是显示另一传统数字权利管理引擎处理的方法步骤流程图。

[0021] 图 3 是显示另一传统数字权利管理引擎处理的方法步骤流程图。

[0022] 图 4 是显示本发明实施例的局部启动数字权利管理引擎的方法步骤流程图。

[0023] 图 5 是显示本发明实施例的局部启动数字权利管理引擎的系统架构示意图。

[0024] 图 6 是显示本发明另一实施例的局部启动数字权利管理引擎的方法步骤流程图。

[0025] 图 7 是显示本发明另一实施例的局部启动数字权利管理引擎的系统架构示意图。

[0026] [主要元件标号说明]

[0027] 500、700 ～存储器装置

[0028] 550、750 ～存储器位置

[0029] 551、751 ～数字内容文件

[0030] 552、752 ～认证码

[0031] 553、753 ～解密钥匙

[0032] 555、755 ～应用程序

[0033] 757 ～权利对象

[0034] 600、800 ～电子装置

[0035] 610、810 ～数字权利管理引擎

[0036] S11..S 15 ～流程步骤

[0037] S21..S27 ～流程步骤

[0038] S31..S 33 ～流程步骤

[0039] S401..S413 ～流程步骤

[0040] S601..S611 ～流程步骤

具体实施方式

[0041] 为了让本发明的目的、特征、及优点能更明显易懂，下文特举较佳实施例，并配合所附图式图 4 至图 7，做详细的说明。本发明说明书提供不同的实施例来说明本发明不同实施方式的技术特征。其中，实施例中的各元件的配置是为说明之用，并非用以限制本发明。且实施例中图式标号的部分重复，是为了简化说明，并非意指不同实施例之间的关联性。

[0042] 本发明实施例揭露了一种局部启动数字权利管理引擎的方法与系统。

[0043] 本发明实施例的局部启动数字权利管理引擎的方法与系统适用于可携式闪存装置（例如，安全数字 (Secure Digital，SD) 存储卡、通用序列总线 (Universal Serial Bus，USB)) 磁盘) 或电子装置中内嵌式闪存装置，用以产生不同于网络系统的数字权利管理机制。该数字权利管理机制利用电子装置的数字权利管理引擎来克服数字权利管理引擎与该电子装置的操作系统间的兼容性问题。

[0044] 图 4 是显示本发明实施例的局部启动数字权利管理引擎的方法步骤流程图。

[0045] 执行前处理操作，其中将权利对象与数字内容文件连接在一起连接在一起 (步骤 S401)，此数字内容文件并有专属的认证码以供验证。将第一文件格式 (例如，OMA 的 .3gp 文件) 的数字内容文件转换为第二文件格式 (例如，OMA DRM 1.0 的 .dm 文件) 的数字内容文件 (步骤 S402)，其仅可被特定电子装置的数字权利管理引擎辨识。举例来说，先以 OMA 1.0 的内容包裹程序 (例如 SONY-Ericsson 的 DRM Packager) 将原始数字内容文件转

换成 .dm 文件，此时权利对象已经和内容被包裹在一起。由于 OMA 的数字权利管理引擎需要经网络传送的程序才能被启动，此 .dm 文件并不能被一般电子装置使用。

[0046] 然而对于已知该工艺流程者，此 .dm 文件可以被拷贝至文件服务器，然后再经网络下载后即可被使用，故必须要有另一层的保护。因此，若自文件服务器下载，则加密该第二文件格式的数字内容文件，其利用加密机制（例如，先进加密系统 (Advanced Encryption System，AES)、3 数据加密系统 (3Data Encryption System，3DES)、双鱼 (Twofish)... 等等）加密该第二文件格式的数字内容文件，其中将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件（例如，.aes 文件），同时产生对应解密钥匙（步骤 S403）。

[0047] 将该加密的数字内容文件与该解密钥匙分别储存在存储器装置（例如，SD 存储卡）的各自存储器位置（例如将数字内容文件储存在公开区，将解密钥匙储存在隐藏区）中（步骤 S404）。该解密钥匙亦可分散储存于该存储器装置或已编译成机器语言的应用程序中而无法被辨识以加强保护。利用程序语言（例如，C++）设计应用程序以执行验证、文件解密、数字权利管理引擎启动与安全控制等操作（步骤 S405），并且将该应用程序安装于该存储器装置上（步骤 S406）。当该存储器装置安装至该电子装置中时（步骤 S407），根据该数字内容文件的认证码对该应用程序进行验证（步骤 S408）。认证码可为该数字内容文件的专属序号或该存储器装置的唯一序号。

[0048] 当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自第三文件格式 (.aes) 的数字内容文件还原至该第二文件格式 (.dm) 的数字内容文件（步骤 S409），并且局部启动该电子装置的数字权利管理引擎（步骤 S410）。该数字权利管理引擎将第二文件格式 (.dm) 的数字内容文件转换为第四文件格式 (.dcf) 的数字内容文件（步骤 S411），并且将该电子装置的内码 (IMEI) 与该数字内容文件连接（权利对象与数字内容文件在前面程序已先行连接在一起）（步骤 S412），使得该数字内容文件仅可被该电子装置存取使用（步骤 S413）。

[0049] 需注意到，当存储器装置自电子装置中移除，或者在该电子装置的数字权利管理引擎启动前关闭该电子装置，该应用程序执行安全控制以删除加密的数字内容文件。

[0050] 图 5 是显示本发明实施例的局部启动数字权利管理引擎的系统架构示意图。

[0051] 该系统包括存储器装置 500 与电子装置 600。电子装置一数字权利管理引擎 630。存储器装置 500 提供存储器位置 550（例如，隐藏区与公开区）以储存数字内容文件 551、数字内容文件 551 的认证码 552、解密钥匙 553 与应用程序 555，其中数字内容文件利 551 用加密方法与解密钥匙 553 来加密。若利用 AES 来处理数字内容文件 551，则数字内容文件 551 的格式为 .aes。

[0052] 利用程序语言（例如，C++）设计应用程序 555 以执行验证、文件解密、数字权利管理引擎启动与安全控制等操作。当存储器装置 500 安装至电子装置 600 时，应用程序 555 根据数字内容文件 551 的认证码 552 进行授权。认证码 552 可为数字内容文件 551 的专属序号或该存储器装置的唯一序号。

[0053] 当成功验证后，应用程序 555 利用解密钥匙 553 解密该加密的数字内容文件 551，其中自第三文件格式 (.aes) 的数字内容文件 551 还原至该第二文件格式 (.dm) 的数字内容文件 551，并且局部启动电子装置 600 的数字权利管理引擎 610。数字权利管理引擎 610 将第二文件格式 (.dm) 的数字内容文件 551 转换为该第一文件格式 (.dcf) 的数字内容文

件 551，并且将电子装置的内码 (IMEI) 与该数字内容文件 551 连接（权利对象与数字内容文件 551 在前面程序已先行连接在一起），使得该数字内容文件 551 仅可被电子装置 600 存取使用。

[0054] 本发明第二实施例揭露了一种局部启动数字权利管理引擎的方法与系统的另外范例。

[0055] 本发明实施例的局部启动数字权利管理引擎的方法与系统适用于可携式闪存装置（例如，安全数字 (Secure Digital，SD) 存储卡、通用序列总线 (Universal Serial Bus，USB)) 磁盘）或电子装置中内嵌式闪存装置，用以产生不同于网络系统的数字权利管理机制。该数字权利管理机制利用电子装置的数字权利管理引擎来克服数字权利管理引擎与该电子装置的操作系统间的兼容性问题。

[0056] 图 6 是显示本发明另一实施例的局部启动数字权利管理引擎的方法步骤流程图。

[0057] 执行前处理操作，将第一文件格式（例如，OMA 的 .3gp 文件）的数字内容文件转换为第二文件格式（例如，OMA DRM 1.0 的 .dcf) 的数字内容文件（步骤 601)，其仅可被特定电子装置的数字权利管理引擎辨识，并且需要结合其相对应的权利对象才能被使用。举例来说，先以 OMA 1.0 的内容包裹程序（例如 SONY-Ericsson 的 DRM Packager) 将原始数字内容文件转换成 .dcf，此时其相对应的权利对象也另外同时产生，但是并不与此第二文件格式的数字内容文件相连接。

[0058] 需注意到，本实施例中的 .dcf 文件与图 4 中的 .dcf 文件不同，其加密时并未使用权利对象。

[0059] 此文件已经过加密处理，基本上没有被非法授权使用的顾虑。但是为增强其保护机制，在本实施中，利用加密机制（例如，先进加密系统 (Advanced Encryption System，AES)、3 数据加密系统 (3Data Encryption System，3DES)、Twofish（双鱼）... 等等）加密该第二文件格式的数字内容文件，其中将该第二文件格式的数字内容文件转换为第三文件格式的数字内容文件（例如，.aes 文件），同时产生对应解密钥匙（步骤 602)。

[0060] 将该加密的数字内容文件与该解密钥匙储存在存储器装置（例如，SD 存储卡）的各自存储器位置（例如将数字内容文件储存在公开区，将解密钥匙储存在隐藏区）中（步骤 603)。该解密钥匙亦可分散储存于该存储器装置或已编译成机器语言的应用程序中而无法被辨识以加强保护。利用程序语言（例如，C++) 设计应用程序以执行验证、文件解密、数字权利管理引擎启动与安全控制等操作（步骤 604)，并且将该应用程序安装于该存储器装置上（步骤 605)。当该存储器装置安装至该电子装置中时（步骤 606)，根据该数字内容文件的认证码对该应用程序进行验证（步骤 607)。认证码可为该数字内容文件的专属序号或该存储器装置的唯一序号。

[0061] 当成功验证后，该应用程序利用该解密钥匙解密该加密的数字内容文件，其中自该第三文件格式 (.aes) 的数字内容文件还原至该第二文件格式 (.dcf) 的数字内容文件（步骤 S608)，并且局部启动该电子装置的数字权利管理引擎（步骤 S609)。该数字权利管理引擎将第二文件格式 (.dcf) 的数字内容文件与权利对象以及该电子装置的内码 (IMEI) 结合，成为同名的第四文件格式 (.dcf) 的数字内容文件（步骤 610)，使得该数字内容文件仅可被该电子装置存取使用（步骤 611)。

[0062] 需注意到，当存储器装置自电子装置中移除，或者在该电子装置的数字权利管理

引擎启动前关闭该电子装置，该应用程序执行安全控制以删除加密的数字内容文件。

[0063] 图 7 是显示本发明另一实施例的局部启动数字权利管理引擎的系统架构示意图。

[0064] 该系统包括存储器装置 700 与电子装置 800。电子装置 800 提供数字权利管理引擎 810。存储器装置 700 提供存储器位置 750（例如，隐藏区与公开区）以储存数字内容文件 751、数字内容文件 751 的认证码 752、解密钥匙 753、应用程序 755、权利对象 757，其中数字内容文件 751 利用加密方法与解密钥匙 753 来加密。若利用 AES 来处理数字内容文件 751，则数字内容文件 751 的格式为 .aes。

[0065] 利用程序语言（例如，C++）设计应用程序 755 以执行验证、文件解密、数字权利管理引擎启动与安全控制等操作。当存储器装置 700 安装至电子装置 800 时，应用程序 755 根据数字内容文件 751 的认证码 752 进行验证。认证码 752 可为数字内容文件 751 的专属序号或存储器装置 700 的唯一序号。

[0066] 当成功验证后，应用程序 755 利用该解密钥匙解密该加密的数字内容文件 751，其中自第三文件格式（.aes）的数字内容文件 751 还原至该第二文件格式（.dcf）的数字内容文件 751，并且局部启动电子装置 800 的数字权利管理引擎 810。数字权利管理引擎 810 将第二文件格式（.dcf）的数字内容文件 751 与权利对象 757 以及电子装置 800 的内码（IMEI）结合，成为同名的第四文件格式（.dcf）的数字内容文件 751，使得该数字内容文件 751 仅可被电子装置 800 存取使用。

[0067] 本发明实施例的局部启动数字权利管理引擎的方法与系统适用于可携式电子装置或可携式快闪存储装置的离线传递，其建立一个可以独立于网络系统之外的数字内容文件与对应的数字权利管理的离线传递。此外，本发明还提供自行设计的应用程序，以启动特定电子装置的数字权利管理引擎，可克服特定电子装置的操作系统与数字权利管理引擎间的兼容性问题。

[0068] 本发明的方法，或特定型态或其部分，可以以程序码的型态存在。程序码可以包含于实体媒体，如软盘、光盘片、硬盘、或是任何其它机器可读取（如计算机可读取）储存媒体，其中，当程序码被机器，如计算机加载且执行时，此机器变成用以参与本发明的装置。程序码也可以通过一些传送媒体，如电线或电缆、光纤、或是任何传输型态进行传送，其中，当程序码被机器，如计算机接收、加载且执行时，此机器变成用以参与本发明的装置。当在一般用途处理单元实作时，程序码结合处理单元提供一操作类似于应用特定逻辑电路的独特装置。

[0069] 虽然本发明已以较佳实施例揭露如上，然其并非用以限定本发明，任何本领域技术人员，在不脱离本发明的精神和范围内，当可作各种的更动与润饰，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。

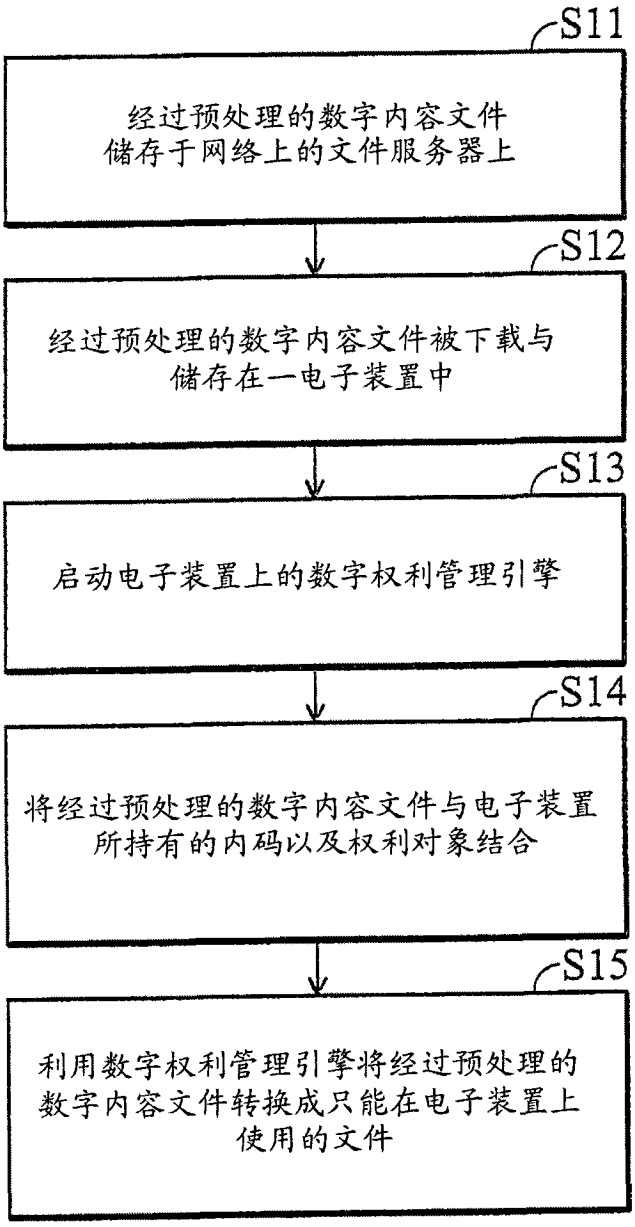

S11
经过预处理的数字内容文件
储存于网络上的文件服务器上
S12
经过预处理的数字内容文件被下载与
储存在一电子装置中
S13
启动电子装置上的数字权利管理引擎
S14
将经过预处理的数字内容文件与电子装置
所持有的内码以及权利对象结合
S15
利用数字权利管理引擎将经过预处理的
数字内容文件转换成只能在电子装置上
使用的文件

图 1

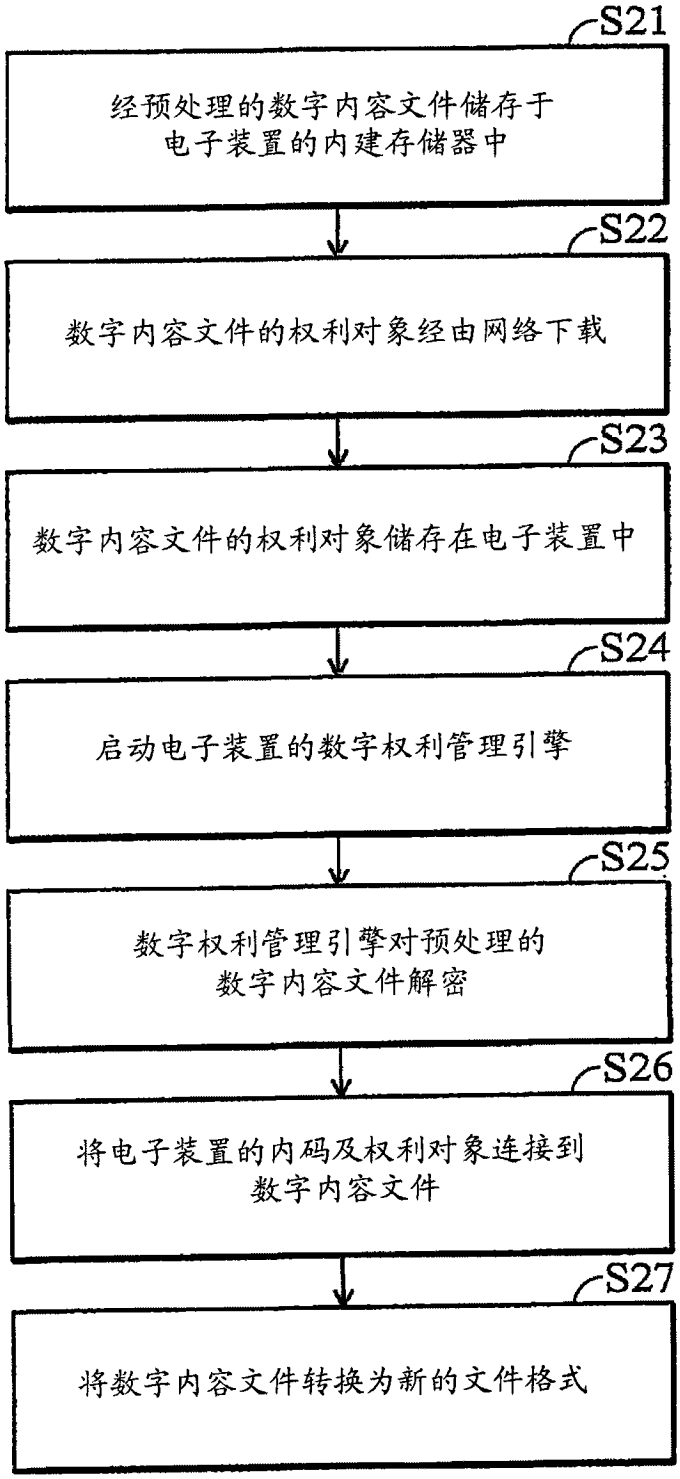

S21
经预处理的数字内容文件储存于电子装置的内建存储器中
S22
数字内容文件的权利对象经由网络下载
S23
数字内容文件的权利对象储存在电子装置中
S24
启动电子装置的数字权利管理引擎
S25
数字权利管理引擎对预处理的数字内容文件解密
S26
将电子装置的内码及权利对象连接到数字内容文件
S27
将数字内容文件转换为新的文件格式

图 2

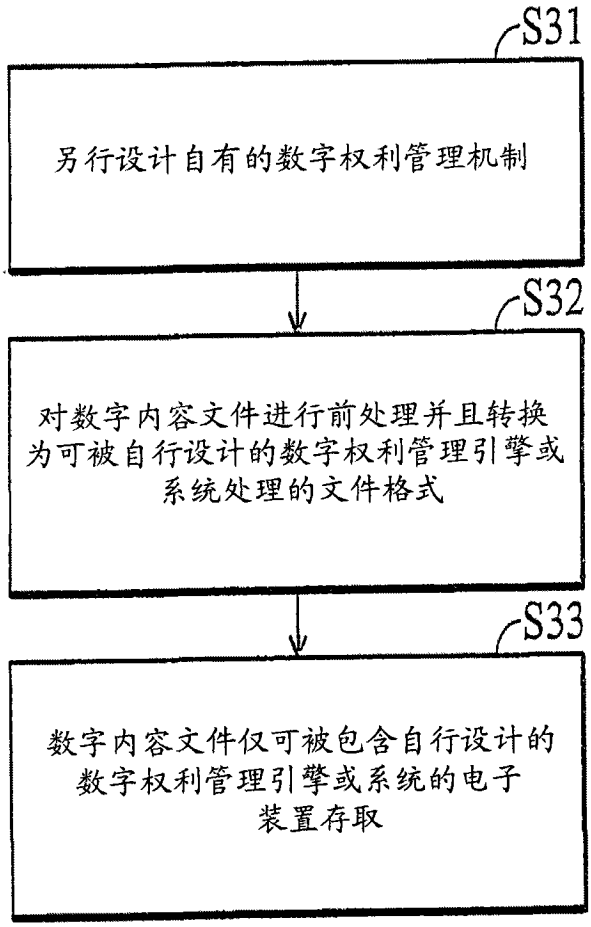

S31
另行设计自有的数字权利管理机制
S32
对数字内容文件进行前处理并且转换为可被自行设计的数字权利管理引擎或系统处理的文件格式
S33
数字内容文件仅可被包含自行设计的数字权利管理引擎或系统的电子装置存取

图 3

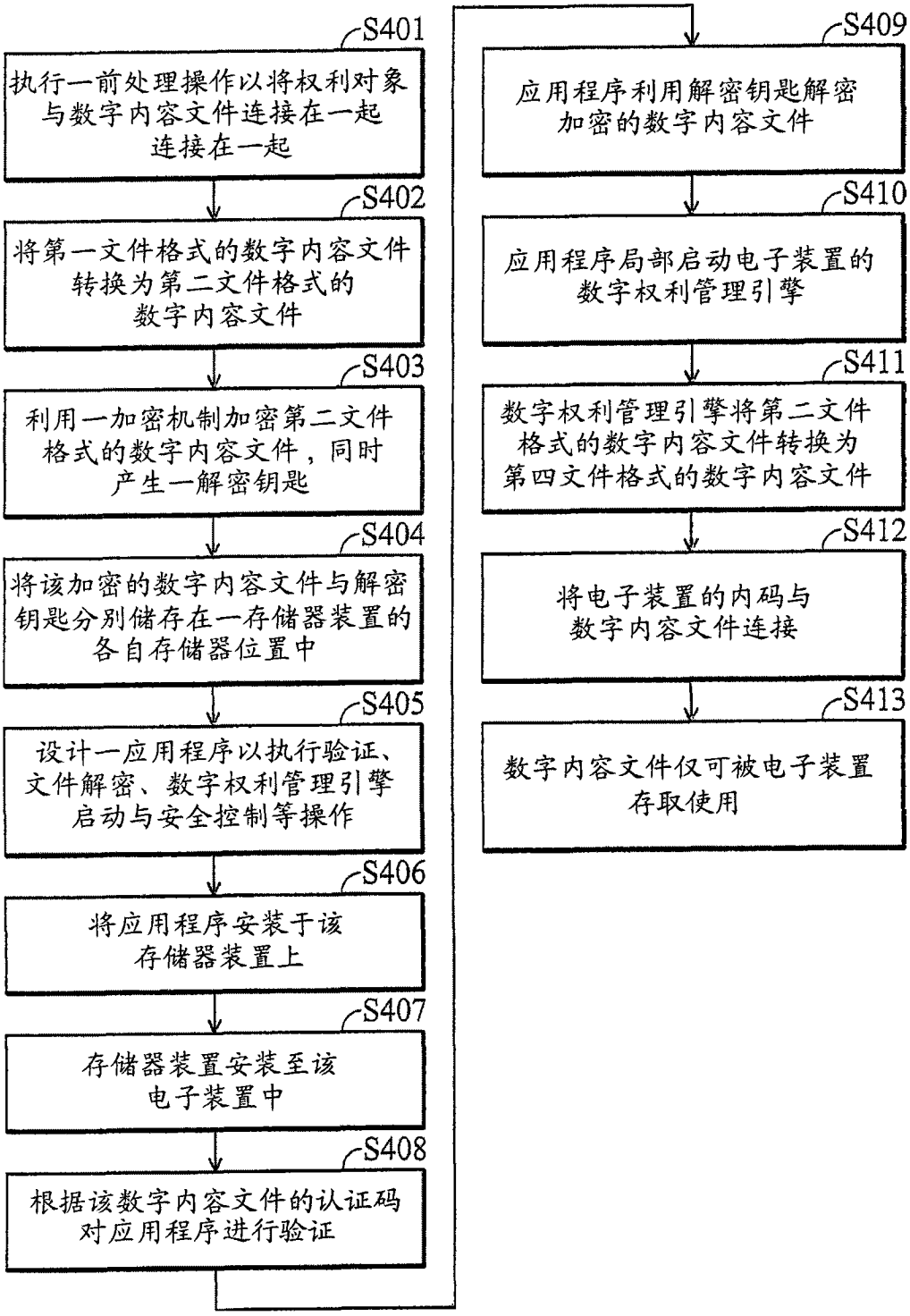

S401
执行一前处理操作以将权利对象与数字内容文件连接在一起连接在一起
S402
将第一文件格式的数字内容文件转换为第二文件格式的数字内容文件
S403
利用一加密机制加密第二文件格式的数字内容文件，同时产生一解密钥匙
S404
将该加密的数字内容文件与解密钥匙分别储存在一存储器装置的各自存储器位置中
S405
设计一应用程序以执行验证、文件解密、数字权利管理引擎启动与安全控制等操作
S406
将应用程序安装于该存储器装置上
S407
存储器装置安装至该电子装置中
S408
根据该数字内容文件的认证码对应用程序进行验证
S409
应用程序利用解密钥匙解密加密的数字内容文件
S410
应用程序局部启动电子装置的数字权利管理引擎
S411
数字权利管理引擎将第二文件格式的数字内容文件转换为第四文件格式的数字内容文件
S412
将电子装置的内码与数字内容文件连接
S413
数字内容文件仅可被电子装置存取使用

图 4

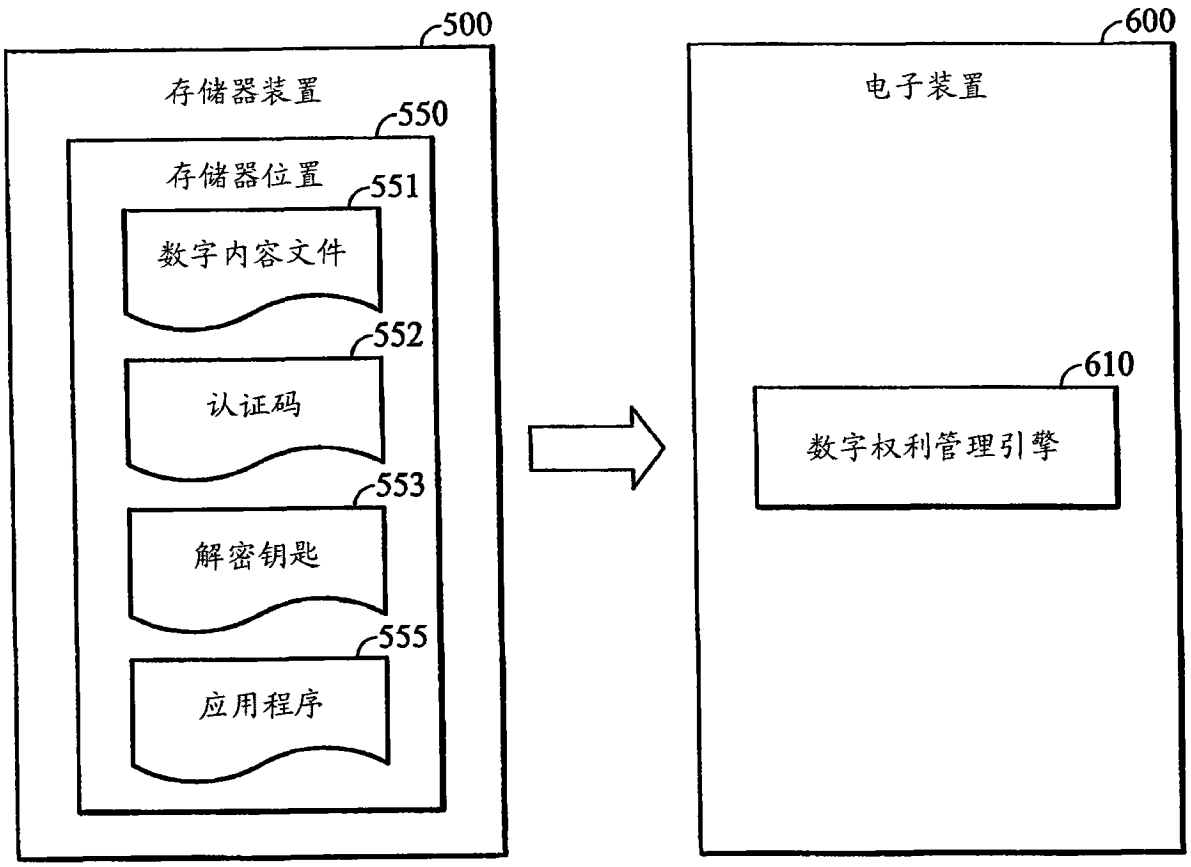

500
存储器装置
550
存储器位置
551
数字内容文件
552
认证码
553
解密钥匙
555
应用程序
600
电子装置
610
数字权利管理引擎

图 5

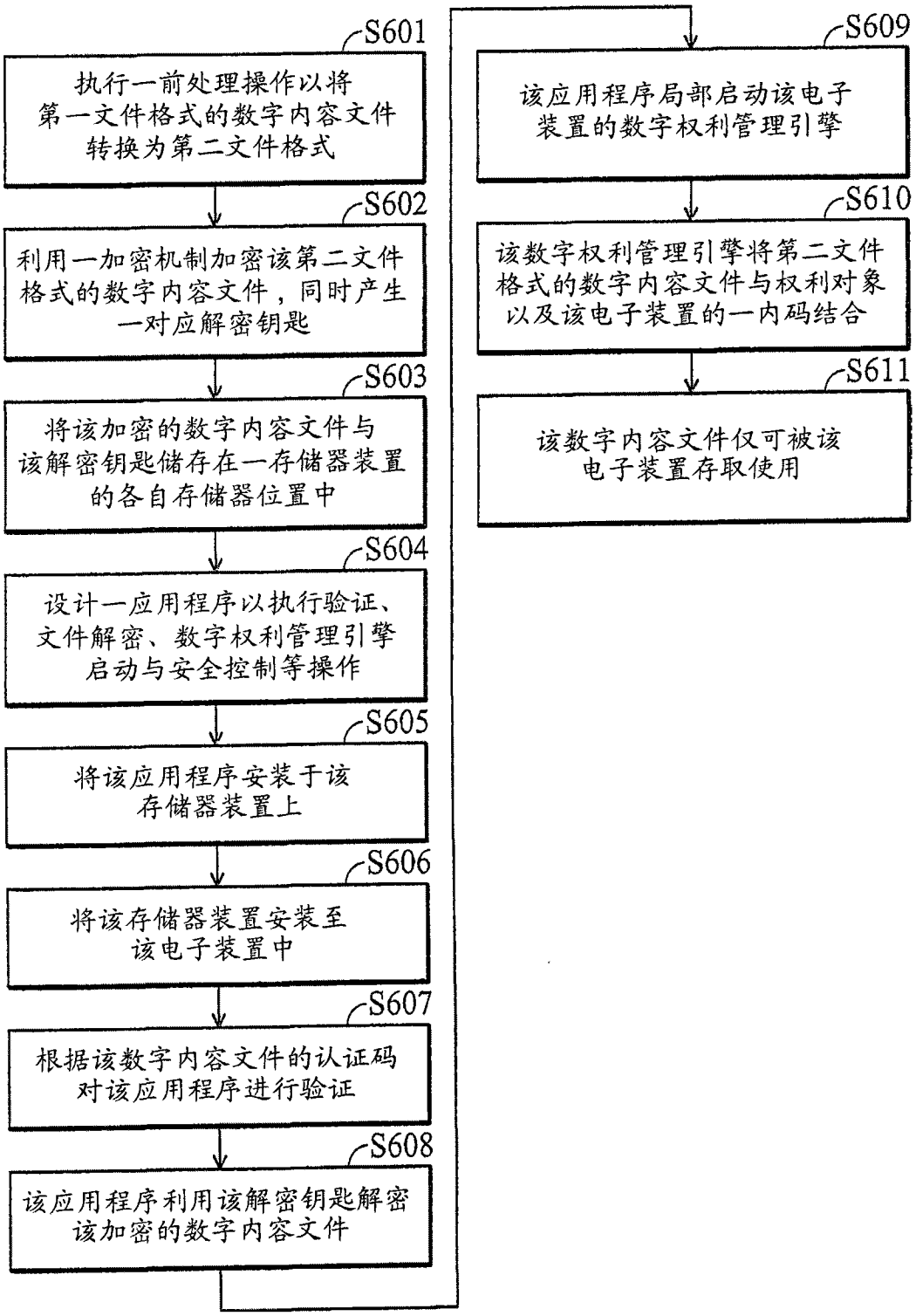

S601
执行一前处理操作以将第一文件格式的数字内容文件转换为第二文件格式
S602
利用一加密机制加密该第二文件格式的数字内容文件，同时产生一对应解密钥匙
S603
将该加密的数字内容文件与该解密钥匙储存在一存储器装置的各自存储器位置中
S604
设计一应用程序以执行验证、文件解密、数字权利管理引擎启动与安全控制等操作
S605
将该应用程序安装于该存储器装置上
S606
将该存储器装置安装至该电子装置中
S607
根据该数字内容文件的认证码对该应用程序进行验证
S608
该应用程序利用该解密钥匙解密该加密的数字内容文件
S609
该应用程序局部启动该电子装置的数字权利管理引擎
S610
该数字权利管理引擎将第二文件格式的数字内容文件与权利对象以及该电子装置的一内码结合
S611
该数字内容文件仅可被该电子装置存取使用

图 6

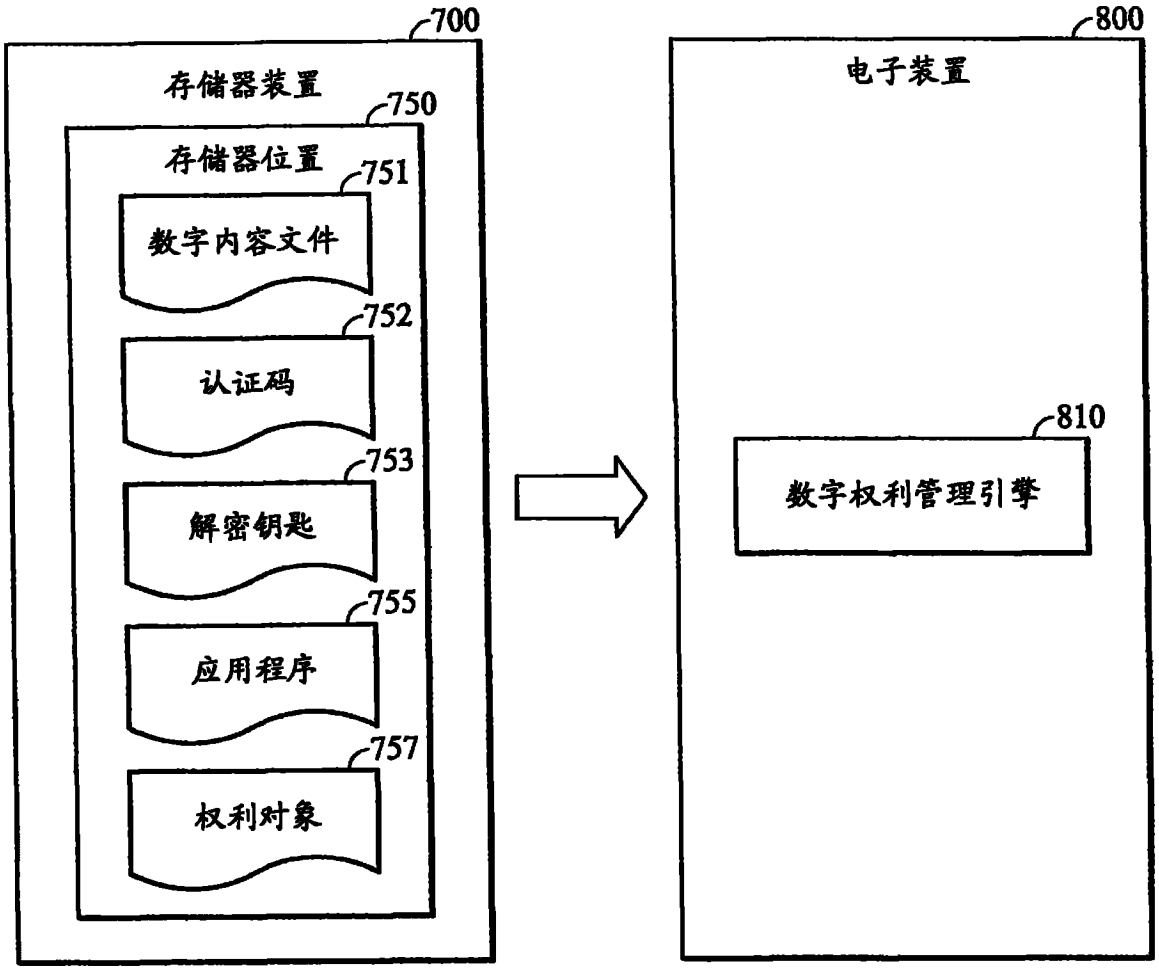

700
存储器装置
750
存储器位置
751
数字内容文件
752
认证码
753
解密钥匙
755
应用程序
757
权利对象
800
电子装置
810
数字权利管理引擎

图 7