[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06F 17/00
G06F 12/14

[12] 发明专利申请公开说明书

[21] 申请号 03153596.8

[43] 公开日 2005 年 2 月 23 日

[11] 公开号 CN 1584870A

[22] 申请日 2003.8.18 [21] 申请号 03153596.8

[71] 申请人 永丰纸业股份有限公司
地址 台湾省台北市
[72] 发明人 黄文贤 郑嘉信 何君毅 徐庸展 邱迪先

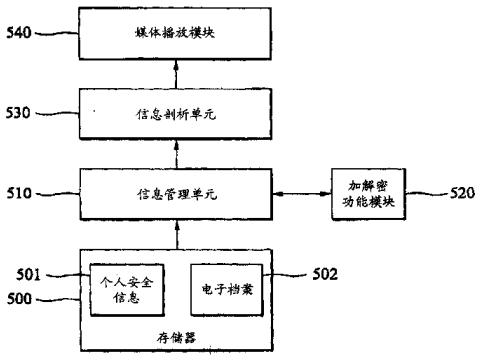
[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 王一斌

权利要求书 5 页 说明书 8 页 附图 6 页

[54] 发明名称 数字内容管理系统与方法及其应用方法

[57] 摘要

一种数字内容管理系统，包括储存个人安全信息与包括加密数字内容与加密对称式金钥的电子档案的存储器、信息管理单元、加解密功能模块、信息剖析模块与媒体播放模块。信息管理单元利用加解密功能模块以个人安全信息对于加密对称式金钥进行解密，从而得到一对称式金钥，且以对称式金钥对于加密数字内容进行解密，从而得到数字内容。信息剖析模块将数字内容进行剖析，从而得到相应的版权控制信息。媒体解析模块可以依据版权控制信息将解密的数字内容进行解析。



ISSN1008-4274

1. 一种数字内容管理系统，包括:

一个人安全信息;

一电子档案，包括一加密数字内容与一加密对称式金钥;

一信息管理单元，以该个人安全信息对于该加密对称式金钥进行解密，从而得到一对称式金钥，且以该对称式金钥对于该加密数字内容进行解密，从而得到一数字内容; 以及

一媒体播放模块，用以将该数字内容进行播放。

2. 根据权利要求 1 所述的数字内容管理系统，其中当该信息管理单元以该对称式金钥对于该加密数字内容进行解密时，更得到相应该数字内容的一发行者的一数字签章，且该信息管理单元更计算相应该数字内容的一第一杂凑值，并取得相应该发行者的一公钥，且依据该公钥解开该数字签章，从而得到一第二杂凑值，并依据该第一杂凑值与该第二杂凑值判断该数字内容是否经过修改。

3. 根据权利要求 2 所述的数字内容管理系统，其中该数字签章是依据相应该发行者的一私钥与相应该数字内容的该第一杂凑值进行制作。

4. 根据权利要求 2 所述的数字内容管理系统，其中相应该发行者的一公钥是记录于相应该发行者的一凭证中，且该凭证记录相应该发行者的身份信息。

5. 根据权利要求 1 所述的数字内容管理系统，其中该加密对称式金钥是依据相应该数字内容的一拥有者的一公钥进行加密。

6. 根据权利要求 1 所述的数字内容管理系统，其中该加密数字内容是依据该对称式金钥进行加密。

7. 根据权利要求 1 所述的数字内容管理系统，更包括一信息剖析

单元，用以将该数字内容进行剖析，从而得到相应该数字内容的一版权控制信息。

8. 根据权利要求 7 所述的数字内容管理系统，其中该数字内容具有复数个档案分区，且每一该等档案分区具有相应的该版权控制信息。

9. 根据权利要求 7 所述的数字内容管理系统，其中该版权控制信息包括相应该数字内容的一授权期限。

10. 根据权利要求 7 所述的数字内容管理系统，其中该版权控制信息包括相应该数字内容的一打印限制信息。

11. 根据权利要求 7 所述的数字内容管理系统，其中该媒体播放模块更依据该版权控制信息播放该数字内容。

12. 根据权利要求 5 所述的数字内容管理系统，其中该个人安全信息是相应该数字内容的该拥有者的一私钥。

13. 根据权利要求 1 所述的数字内容管理系统，其中该个人安全信息与该电子档案是储存于一可携式储存装置中。

14. 一种数字内容管理方法，包括下列步骤:

提供包括一加密数字内容与一加密对称式金钥的一电子档案;

以一个人安全信息对于该加密对称式金钥进行解密,从而得到一对称式金钥;

以该对称式金钥对于该加密数字内容进行解密，从而得到一数字内容; 以及

以一媒体播放模块将该数字内容进行播放。

15. 根据权利要求 14 所述的数字内容管理方法，其中当以该对称式金钥对于该加密数字内容进行解密时，更得到相应该数字内容的一发行者的一数字签章，且更包括下列步骤:

计算相应该数字内容的一第一杂凑值;

取得相应该发行者的一公钥;

依据该公钥解开该数字签章，从而得到一第二杂凑值；以及

依据该第一杂凑值与该第二杂凑值判断该数字内容是否经过修改。

16. 根据权利要求 15 所述的数字内容管理方法，其中该数字签章是依据相应该发行者的一私钥与相应该数字内容的该第一杂凑值进行制作。

17. 根据权利要求 15 所述的数字内容管理方法，其中相应该发行者的一公钥是记录于相应该发行者的一凭证中，且该凭证记录相应该发行者的身份信息。

18. 根据权利要求 14 所述的数字内容管理方法，其中该加密对称式金钥是依据相应该数字内容的一拥有者的一公钥进行加密。

19. 根据权利要求 14 所述的数字内容管理方法，其中该加密数字内容是依据该对称式金钥进行加密。

20. 根据权利要求 14 所述的数字内容管理方法，更包括将该数字内容进行剖析，从而得到相应该数字内容的一版权控制信息。

21. 根据权利要求 20 所述的数字内容管理方法，其中该数字内容具有复数个档案分区，且每一该等档案分区具有相应的该版权控制信息。

22. 根据权利要求 20 所述的数字内容管理方法，其中该版权控制信息包括相应该数字内容的一授权期限。

23. 根据权利要求 20 所述的数字内容管理方法，其中该版权控制信息包括相应该数字内容的一打印限制信息。

24. 根据权利要求 20 所述的数字内容管理方法，更包括以该媒体播放模块依据该版权控制信息播放该数字内容。

25. 根据权利要求 18 所述的数字内容管理方法，其中该个人安全信息是相应该数字内容的该拥有者的一私钥。

26. 根据权利要求 14 所述的数字内容管理方法，其中该个人安全信息与该电子档案是储存于一可携式储存装置中。

27.一种数字内容应用方法，适用于一数字内容应用平台，包括下列步骤：

一发行者将一数字内容制作一数字签章；

该发行者将具有该数字签章的该数字内容传送至该数字内容应用平台的一数字内容网站管理后台；

该数字内容网站管理后台验证该数字内容，以判定相应该数字内容的该发明者与一完整性信息；以及

该数字内容网站管理后台将该数字内容储存至一数字内容档案服务器。

28. 根据权利要求27所述的数字内容应用方法，更包括下列步骤：

一消费者于该数字内容应用平台选定该数字内容；

该数字内容应用平台由该数字内容档案服务器取得该数字内容；

该数字内容应用平台由一认证服务器取得相应该消费者的一凭证；

该数字内容应用平台将该数字内容与该凭证传送至一加密服务器；

该加密服务器以一对称式金钥将该数字内容进行加密，从而得到一加密数字内容；

该加密服务器依据该凭证将该对称式金钥进行加密，从而得到一加密对称式金钥；以及

该数字内容应用平台将该加密数字内容与该加密对称式金钥结合为一电子档案，并将该电子档案传送至该消费者。

29. 根据权利要求27所述的数字内容应用方法，其中该发行者将该数字内容进行数字签章的方法，包括下列步骤：

计算该数字内容的一杂凑值；以及

依据相应该发行者的一私钥与该杂凑值制作该数字签章。

30. 根据权利要求27所述的数字内容应用方法，其中该数字内容网站管理后台验证该数字内容的方法，包括下列步骤：

计算相应该数字内容的一第一杂凑值；

取得相应该发行者的一公钥；

依据该公钥解开该数字签章，从而得到一第二杂凑值；以及

依据该第一杂凑值与该第二杂凑值判断该数字内容是否经过修改。

31. 根据权利要求 28 所述的数字内容应用方法，更包括下列步骤：

该消费者以相应该消费者的一私钥对于该加密对称式金钥进行解密，从而得到该对称式金钥；

以该对称式金钥对于该加密数字内容进行解密，从而得到该数字内容；以及

以一媒体播放模块将该数字内容进行播放。

32. 根据权利要求 31 所述的数字内容应用方法，更包括下列步骤：

将该数字内容进行剖析，从而得到相应该数字内容的一版权控制信息；以及

以该媒体播放模块依据该版权控制信息播放该数字内容。

33. 根据权利要求 32 所述的数字内容应用方法，其中该数字内容具有复数个档案分区，且每一该等档案分区具有相应的该版权控制信息。

34. 根据权利要求 32 所述的数字内容应用方法，其中该版权控制信息包括相应该数字内容的一授权期限。

35. 根据权利要求 32 所述的数字内容应用方法，其中该版权控制信息包括相应该数字内容的一打印限制信息。

数字内容管理系统与方法及其应用方法

技术领域

本发明是有关于一种数字内容管理系统及方法，且特别有关于一种可以针对数字内容进行有效的版权控管，且提供数字内容进行应用的系统与方法。

背景技术

随着计算机与网络的普及，人们的生活型态已经面临重大改变。举例来说，数字内容的建立与管理已经取代传统的数据记录型态，且因特网已经成为人们收集数据的最佳方式。此外，人们也尝试由因特网进行商业应用，如购物与下载相关信息与档案等等。同时，随着数据记录与传播型态的改变，数字内容，如电子书与影音文件等数据也已经成为生活中重要的传播方式之一。

目前针对数字内容进行版权控管的方式是将数字内容进行加密之后，再提供给购买者依据其安全信息，如密码或是私钥(Private Key)将其解密，以得到原始的数字内容并进行解析。习知的方法中，由于数字内容是储存于计算机之中，而安全信息是储存于芯片卡或是计算机之中，当使用者欲解析数字内容时，必须将安全信息汇入储存数字内容的计算机之中，且计算机必须具有解密能力方可对于数字内容进行解析。而当使用者欲于不同的计算机主机解析时，则又必须将安全信息与数字内容复制至此计算机主机中，并于计算机主机中安装解密软件方可进行解析。

由于电子数字内容的易复制性且缺乏有效的控管机制，数字内容极易

被使用者复制与盗用，造成数字内容著作权管理上的困难，也无法对于数字内容的版权进行有效控管，进而阻碍数字内容产业与市场的发展与成长。

发明内容

本发明的主要目的为提供一种可以对于数字内容进行有效版权控管的数字内容管理系统及方法。

本发明的另一目的为提供一种可以于网络进行数字内容应用的数字内容交换方法。

为了达成上述目的，可借由本发明的数字内容管理系统与方法及其应用方法达成。依据本发明实施例的数字内容管理系统，包括一个人安全信息、包括一加密数字内容与一加密对称式金钥的一电子档案、一信息管理单元与一媒体播放模块。信息管理单元以个人安全信息对于加密对称式金钥进行解密，从而得到一对称式金钥，且以对称式金钥对于加密数字内容进行解密，从而得到一数字内容。媒体播放模块可以将解密的数字内容进行播放。

当信息管理单元以对称式金钥对于加密数字内容进行解密时，更得到相应数字内容的一发行者的一数字签章，且信息管理单元更计算相应数字内容的一第一杂凑值，并取得相应发行者的一公钥，且依据公钥解开数字签章，从而得到一第二杂凑值，并依据第一杂凑值与第二杂凑值判断数字内容是否经过修改。

数字内容管理系统更包括一信息剖析单元，用以将数字内容进行剖析，从而得到相应数字内容的版权控制信息。其中，数字内容可以具有多个档案分区，且每一档案分区具有相应的版权控制信息，且媒体播放模块可以依据版权控制信息播放此数字内容。

在一最佳情况下，个人安全信息与电子档案是储存于一可携式储存装

置中。

依据本发明实施例的数字内容应用的一范例－应用方法。首先，发行者将数字内容进行数字签章，且将具有数字签章的数字内容传送至网络上一数字内容应用平台的数字内容网站管理后台。之后，数字内容网站管理后台验证数字内容，以判定相应数字内容的发明者与完整性信息。然后，数字内容网站管理后台将数字内容储存至数字内容档案服务器。

当消费者欲购买数字内容时，消费者于数字内容应用平台选定数字内容。之后，数字内容应用平台由数字内容档案服务器取得数字内容，并由认证服务器取得相应消费者的凭证。然后，数字内容应用平台将数字内容与凭证传送至加密服务器。加密服务器以对称式金钥将数字内容进行加密，从而得到加密数字内容，且依据凭证将对称式金钥进行加密，从而得到一加密对称式金钥。最后，数字内容应用平台将加密数字内容与加密对称式金钥结合为一电子档案，并将其传送至消费者。

附图说明

图 1 为一示意图是显示依据本发明实施例的数字内容的应用环境；

图 2 为一流程图是显示依据本发明实施例的数字内容的数字签章流程；

图 3 为一流程图是显示依据本发明实施例的验证数字内容的发行者身分与完整性的流程；

图 4 为一流程图是显示依据本发明实施例的对于数字内容加密的流程；

图 5 为一示意图是显示依据本发明实施例的数字内容管理系统的系统架构；

图 6 为一流程图是显示依据本发明实施例的数字内容解密与播放流

程。

符号说明:

100-数字内容应用平台

101-数字内容网络管理后台

102-数字内容档案服务器

103-认证服务器

104-加密服务器

110-消费者

120-发行者

130-网络

S201、S202-操作步骤

S301、S302、...、S306-操作步骤

S401、S402、...、S405-操作步骤

500-存储器

501-个人安全信息

502-电子档案

510-信息管理单元

520-加解密功能模块

530-信息剖析单元

540-媒体播放模块

S601、S602、...、S605-操作步骤

具体实施方式

如图 1 所示，是显示依据本发明实施例的数字内容的应用环境。如图所示，数字内容的应用环境包括消费者 110 与数字内容的发行者 120，且

其可以透过网络 130 与数字内容应用平台 100 耦接。注意的是，数字内容可以是电子文件、或是影音文件等数字电子数据。

数字内容应用平台100为一平台来提供消费者110与发行者120进行数字内容的应用。数字内容应用平台 100 中包括一数字内容网络管理后台 101、一数字内容档案服务器 102、一认证服务器 103 与一加密服务器 104。每一单元的详细操作将于后进行说明。值得注意的是，本发明可以建构一公钥基础建设，并对每一数字内容的发行者、代理者与拥有者分别发予一凭证，以让发行者可利用此凭证对此档案作数字签章，并将数字内容用拥有者的凭证加密，以防止被他人所解析。其中，所有的凭证信息都可以于认证服务器 103 中记录。

图2是显示依据本发明实施例发行者120对于数字内容的数字签章流程。发行者 120 取得数字内容之后，如步骤 S201，依据一杂凑函式(Hash Function)计算此数字内容的杂凑值。之后，取得发行者 120 的私钥，并如步骤 S202，依据发行者 120 的私钥与数字内容的杂凑值制作数字签章，以完成具有数字签章的数字内容。值得注意的是，本发明的数字签章是利用非对称式金钥的技术，以确保数字内容的完整性、不可否认性与鉴定性。

当发行者 120 对于数字内容进行数字签章之后，将发行者 120 可以登入数字内容应用平台 100，并将具有数字签章的数字内容传送至数字内容应用平台 100 内的数字内容网站管理后台 101 之中。

图3是显示依据本发明实施例的数字内容网站管理后台101验证数字内容的发行者身分与完整性的流程。当数字内容网站管理后台 101 接收到数字内容之后，如步骤 S301，依据杂凑函式直接计算数字内容的第一杂凑值。接着，如步骤 S302，数字内容网站管理后台 101 取得数字内容的凭证，并依据凭证内所记载的发行者 120 的身份信息来确认发行者身份。之后，数字内容网站管理后台 101 取得凭证内相应发行者 120 的公

钥，并如步骤 S303，依据发行者 120 的公钥解开相应数字内容的数字签章，从而得到一第二杂凑值。

之后，如步骤 S304，数字内容网站管理后台 101 比对第一杂凑值与第二杂凑值。当第一杂凑值与第二杂凑值不同时(步骤 S304 的否)，则如步骤 S305，代表数字内容已经被修改过(不具完整性)。而当第一杂凑值与第二杂凑值相同时(步骤 S304 的是)，则如步骤 S306，代表此数字内容是完整地。因此，数字内容网站管理后台 101 可以将此数字内容储存至数字内容档案服务器 102 中。

如前所述，数字内容可以利用拥有者的凭证加密，以防止被他人所解析或盗用。因此，当消费者 110 于数字内容应用平台 100 选定欲购买下载的数字内容之后，数字内容应用平台 100 由数字内容档案服务器 102 取得指定的数字内容，且由认证服务器 103 取得相应消费者 110 的凭证。之后，数字内容应用平台 100 将数字内容与凭证传送至加密服务器 104，以进行相关加密作业。

第 4 图是显示依据本发明实施例的加密服务器 104 对于数字内容加密的流程。首先，如步骤 S401，加密服务器 104 以随机方式产生一对称式金钥，并如步骤 S402，以此对称式金钥将数字内容进行加密，从而产生一加密数字内容。之后，如步骤 S403，加密服务器 104 取得凭证中相应消费者 110 的公钥，并如步骤 S404，利用消费者 110 的公钥将对称式金钥进行加密，从而得到一加密对称式金钥。最后，如步骤 S405，加密服务器 104 将加密数字内容与加密对称式金钥结合为一电子档案。

当加密服务器 104 完成加密作业而产生相应的电子档案之后，数字内容应用平台 100 可以将此电子档案传送给消费者 110。值得注意的是，数字内容应用平台 100 可以依据消费者 110 对于此数字内容的购买情况，进行版权控制信息的产生。其中，版权控制信息可以包括相应数字内容的授权期限、打印限制信息、发行者信息、数字签章等等。此外，数字

内容亦可区分为多个档案分区，且每一档案分区具有相应的版权控制信息来控制该档案分区内数字内容的播放版权。此外，数字内容应用平台100可以将版权控制信息结合于加密数字内容中。在一情况下，版权控制信息可以利用可扩展标记语言(Extensible Markup Language，XML)来呈现。另一方面，数字内容应用平台100对于消费者110购买数字内容的行为亦有相应的计费与请款机制，然其并非本案的主要特征，因此在此省略。

图5是显示依据本发明实施例的消费者端的数字内容管理系统的系统架构。如图所示，依据本发明实施例的数字内容管理系统，包括一存储器500、一信息管理单元510、一加解密功能模块520、一信息剖析模块530与一媒体播放模块540。

存储器500中储存消费者110的个人安全信息501，如私钥与包括加密数字内容与加密对称式金钥的电子档案502。其中，电子档案502是由数字内容应用平台100所购买与下载。信息管理单元510可以将加密数字内容解密还原为数字内容，其操作将于后详细说明。加解密功能模块520可以提供密码学演算的应用程序，如对称式及非对称式金钥的加/解密及签/验章等功能。信息剖析模块530可以对于数字内容进行剖析，从而得到相应的数字内容与版权控制信息。媒体播放模块540可以是文字阅读器或是影音播放器或是任何媒体解析器等，用以将数字内容进行播放。

图6是显示依据本发明实施例的数字内容解密与播放流程。当消费者110(数字内容的拥有者)欲读取数字内容时，如步骤S601，信息管理单元510由存储器500中取得相应消费者110的私钥(个人安全信息501)，并如步骤S602，信息管理单元510依据加解密功能模块520提供的功能利用消费者110的私钥对于加密对称式金钥进行解密，从而得到对称式金钥。

接着，如步骤 S603，信息管理单元 510 利用对称式金钥对于加密数字内容进行解密，从而得到解密之后的数字内容。之后，如步骤 S604，信息剖析模块 530 将数字内容进行剖析，从而得到相应此数字内容的版权控制信息。然后，如步骤 S605，媒体播放模块 540 可以依据版权控制信息将解密的数字内容进行播放。值得注意的是，信息管理单元 510 亦可对于数字内容进行验证，即验证数字内容的发行者身分与完整性，其方法如图 3 所示。

特别需要注意的是，为了强化数字内容版权控管与著作权管理的有效性，消费者的个人安全信息、媒体播放模块与电子档案可以存放于可携式储存装置，如随身碟中。透过此技术的辅助，可使数字内容拥有者可随时携带此可携式储存装置，于每一台计算机解析与读取数字内容。

因此，借由本发明所提出的数字内容管理系统与方法及其应用方法，可以提供数字内容的创新应用模式且对于数字内容进行有效版权控管。此外，在传输过程中，数字内容可被确认其发行者的身分，并确保其内容未被窜改，也不会被非拥有者所解析。

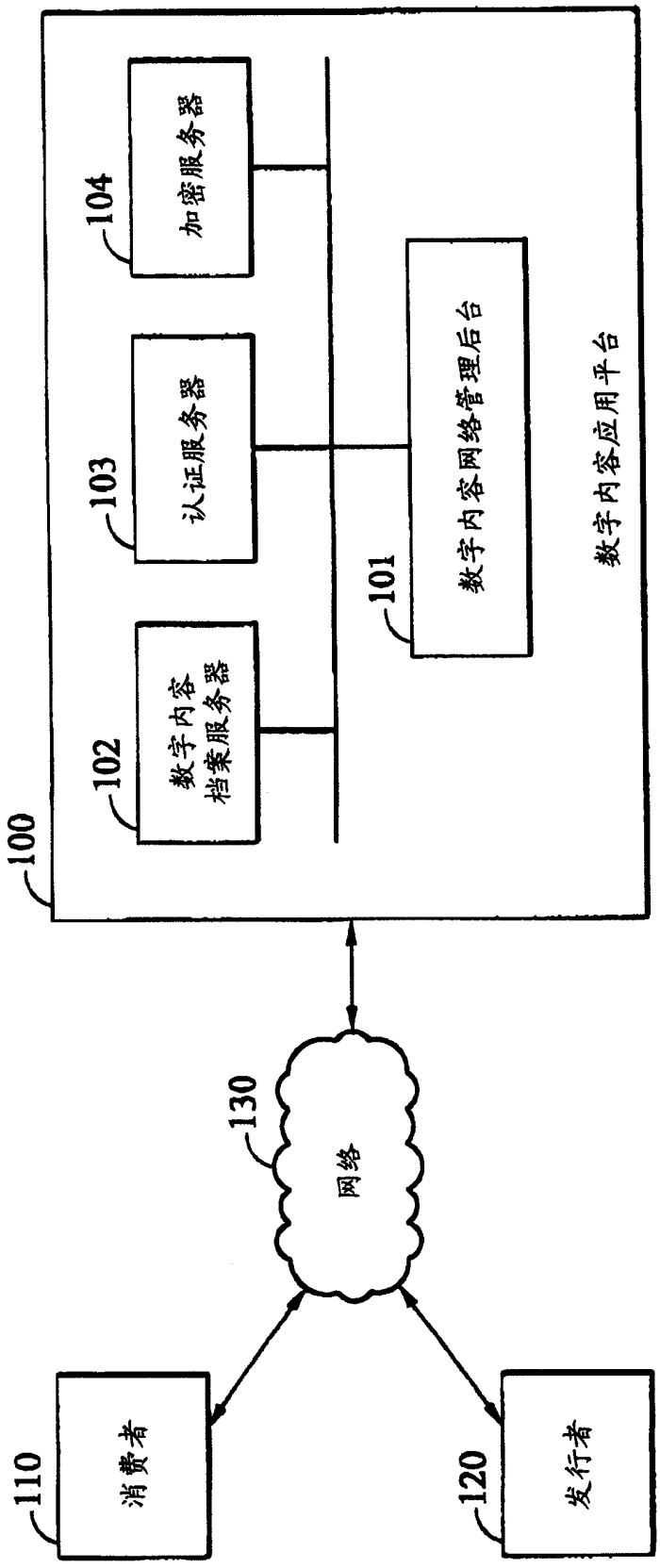

100
数字内容应用平台
101
数字内容网络管理后台
102
数字内容
档案服务器
103
认证服务器
104
加密服务器
130
网络
110
消费者
120
发行者

图1

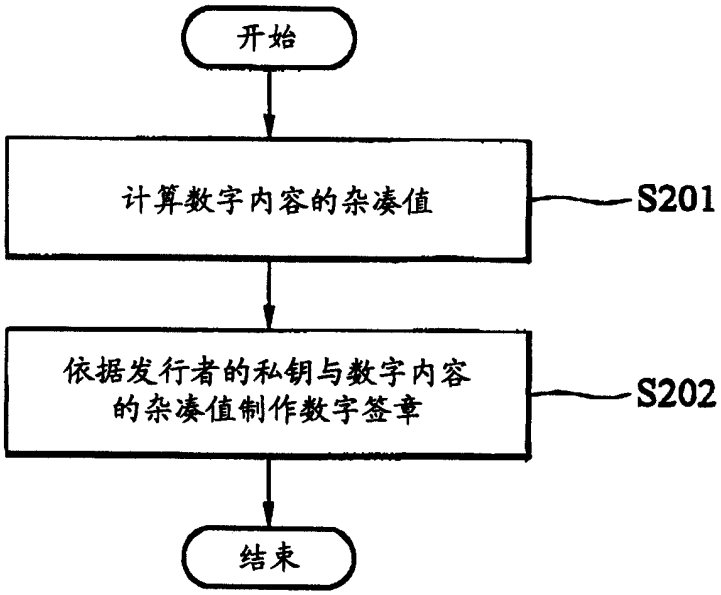


图2

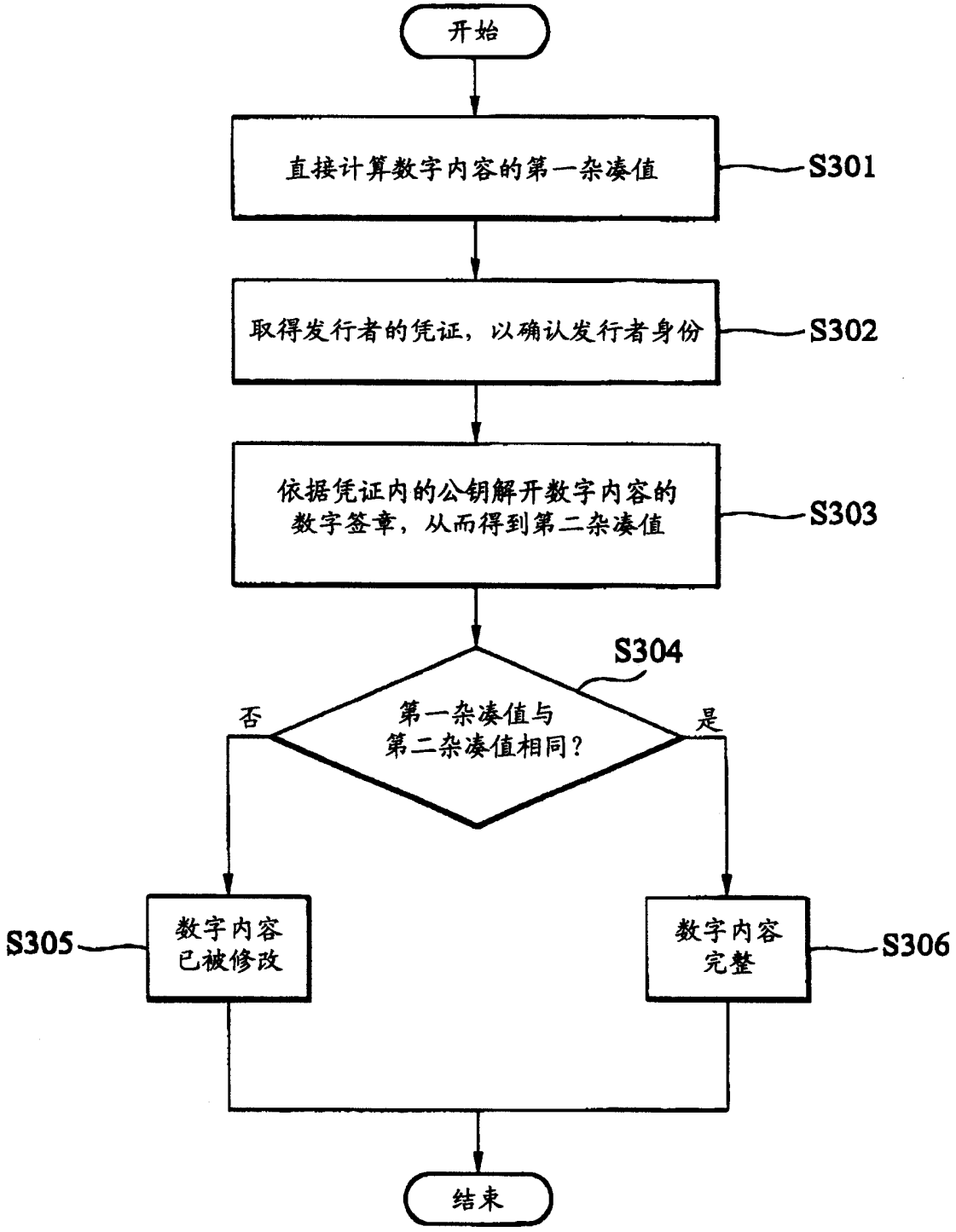

开始
直接计算数字内容的第一杂凑值
S301
取得发行者的凭证，以确认发行者身份
S302
依据凭证内的公钥解开数字内容的
数字签章，从而得到第二杂凑值
S303
S304
第一杂凑值与
第二杂凑值相同？
否
是
S305
数字内容
已被修改
数字内容
完整
S306
结束

图3

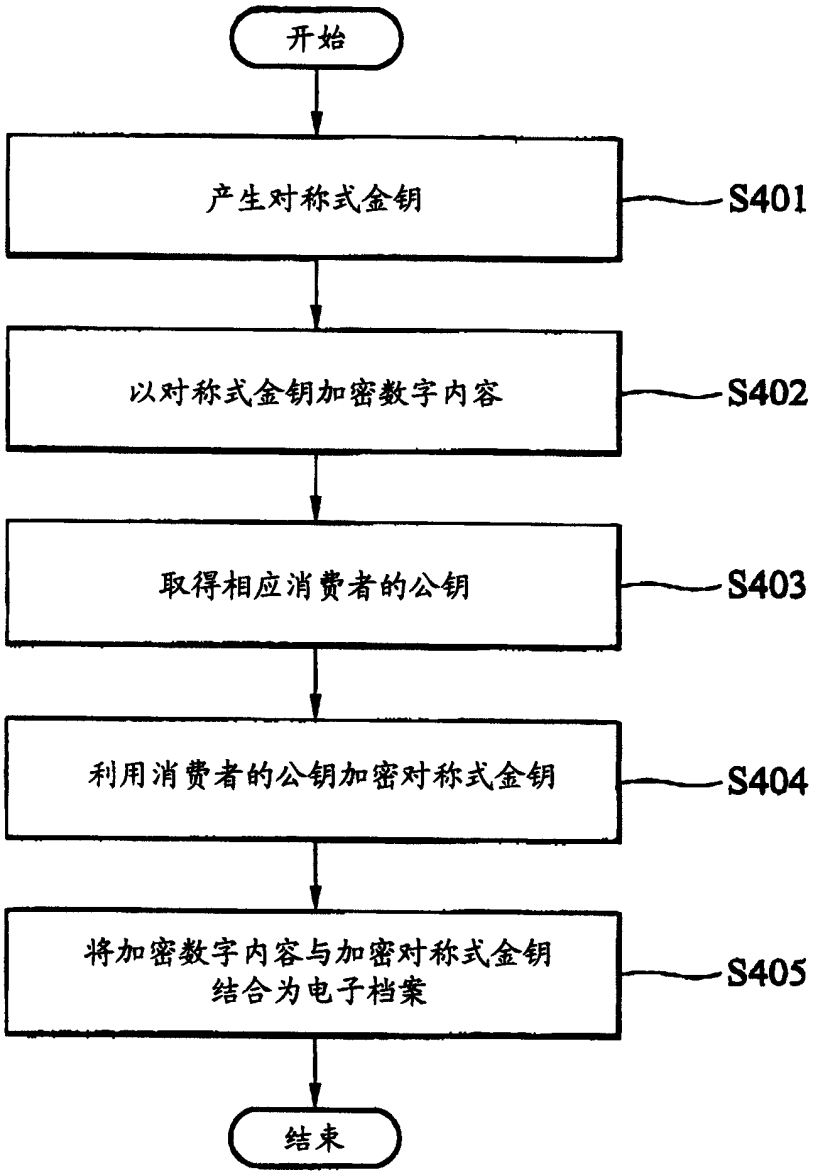

开始
产生对称式金钥
S401
以对称式金钥加密数字内容
S402
取得相应消费者的公钥
S403
利用消费者的公钥加密对称式金钥
S404
将加密数字内容与加密对称式金钥
结合为电子档案
S405
结束

图4

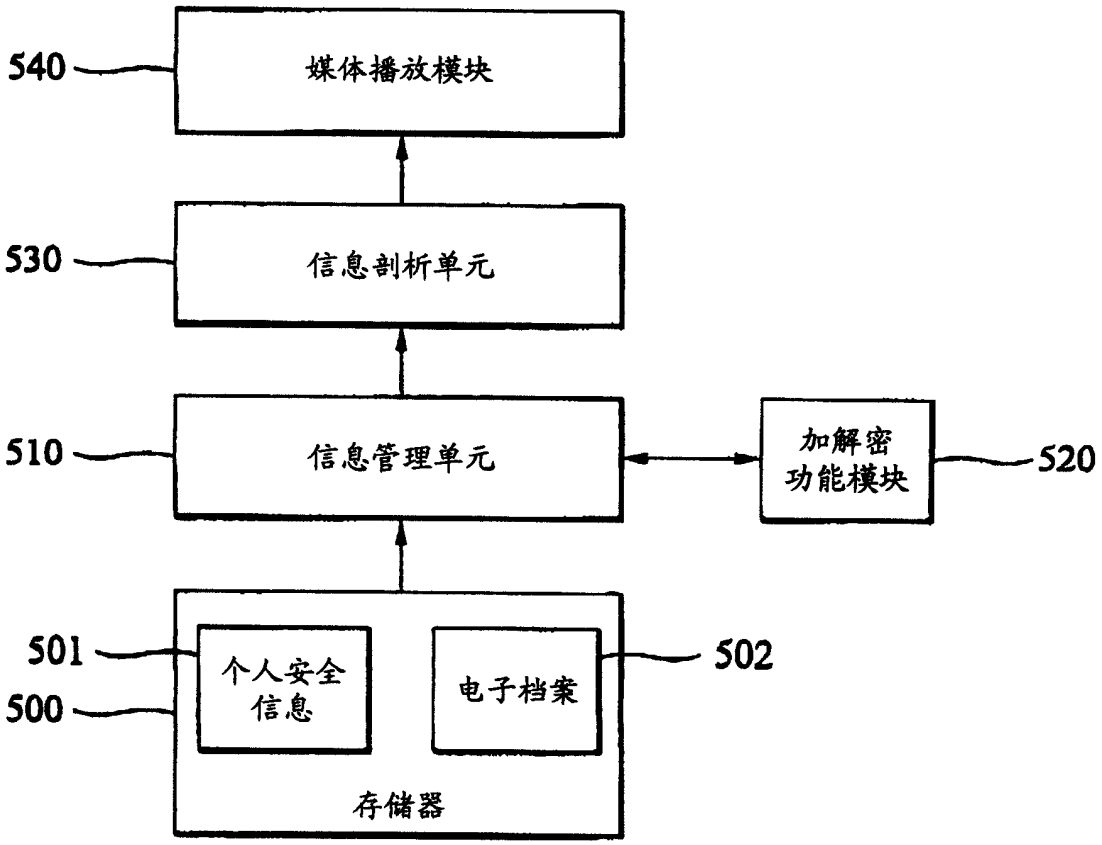

540
媒体播放模块
530
信息剖析单元
510
信息管理单元
加解密
功能模块
520
501
500
个人安全
信息
电子档案
502
存储器

图5

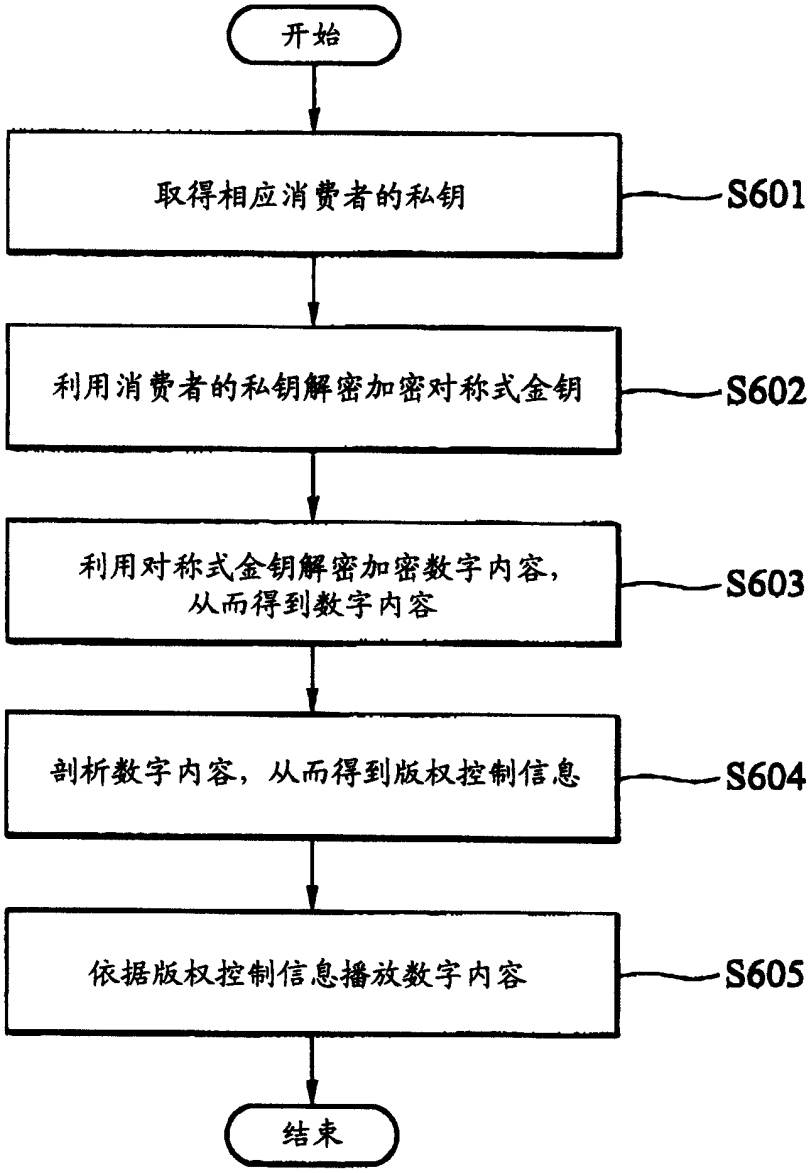

开始
取得相应消费者的私钥
S601
利用消费者的私钥解密加密对称式金钥
S602
利用对称式金钥解密加密数字内容，
从而得到数字内容
S603
剖析数字内容，从而得到版权控制信息
S604
依据版权控制信息播放数字内容
S605
结束

图6