[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/00

[12] 发明专利说明书

[21] ZL 专利号 96121024.9

[43] 授权公告日 2003 年 6 月 4 日

[11] 授权公告号 CN 1110922C

[22] 申请日 1996.11.19 [21] 申请号 96121024.9

[30] 优先权

[32] 1996. 5.20 [33] JP [31] 124823/1996

[71] 专利权人 富士通株式会社

地址 日本神奈川

[72] 发明人 秋山良太 吉冈诚 内田好昭

[56] 参考文献

EP0302710A2 1989.02.08 G06F1/00

US4658093A 1987.04.14 H04L9/00

审查员 董泽华

[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所

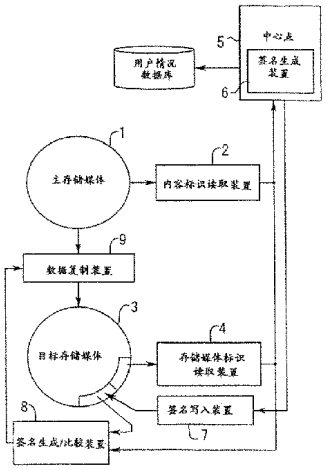
代理人 吴丽丽

权利要求书 5 页 说明书 12 页 附图 10 页

[54] 发明名称 软件复制系统和方法

[57] 摘要

软件复制系统，其中：内容标识读取单元从主存储媒介中读出/软件标识，存储媒介标识读取单元从目标存储媒介中读出存储媒介标识。 两个标识被送往管理软件产品复制权许可的中心点。 在此，签名生成单元根据标识产生第一签名并将其返回用户端。 签名生成/比较单元根据与送往中心点的相同的标识产生第二签名，并把它与储存在目标存储媒介中的第一签名作比较，判断是否进行软件复制。



ISSN1008-4274

1. 一个软件复制系统，用于在合法状态下，通过在请求许可复制软件的终端用户和管理许可的中心点之间的通信，将记录在主存储媒介中的软件复制到目标存储媒介中去，所述软件复制系统包括：

内容标识读取设备，从主存储媒介中读出第一标识，所述的第一标识是唯一地分配给记录在主存储媒介中的软件程序的；

存储媒介标识读取设备，从目标存储媒介中读出第二标识，第二标识是唯一分配给目标存储媒介的；

签名生成设备，设在中心点，根据所述内容标识读取设备读出的第一标识和所述存储媒介标识读取设备读出的第二标识，生成第一签名，该第一签名用作软件程序复制许可的证实；

签名写入设备，将所述签名生成设备生成的第一签名写入目标存储媒介；

签名生成/比较设备，出于验证的目的，根据所述内容标识读取设备读出的第一标识和所述存储媒介标识读取设备读出的第二标识生成一个第二签名，并对储存在目标存储媒介中的第一签名和该第二签名进行比较；

数据复制设备，当所述签名生成/比较设备进行比较的结果证实第一和第二标识相同时，从主存储媒介中检索出软件程序并将软件程序写入目标存储媒介中。

2. 依据权利要求 1 的软件复制系统，其中，所述的签名生成设备包括：

签名处理设备，用一个由中心点管理的检验关键码对所述内容标识读取设备读出的第一标识和所述存储媒介标识读取设备读出的第二标识进行加密，来生成一个作为第一签名使用的检验代码；和

加密设备，用一个在中心点登记过的用户关键码对检验关键码加密，并为在所述的签名生成/比较设备中生成第二签名而发送加

密过的检验关键码。

并且其中所述的签名生成/比较设备包括:

解密设备,用在中心点登记的用户关键码对加密的检验关键码解密,生成一个解密的检验关键码,

检验代码生成设备,为了验证的目的,用解密的检验关键码对所述内容标识读取设备读出的第一标识和所述存储媒介标识读取设备读出的第二标识加密,生成另一个检验代码,作为第二签名使用;和

比较设备,对为了验证而由所述检验代码生成设备生成的检验代码和储存在目标存储媒介中作为第一签名的检验代码作比较。

3. 一种软件复制方法,用于在合法状态下,通过在请求许可复制软件的终端用户和管理许可的中心点之间的通信,将记录在主存储媒介中的软件复制到目标存储媒介中去,软件复制方法包括以下步骤:

从终端用户方向中心点发送一个唯一分配给目标存储媒介的存储媒介标识和一个唯一分配给主题数据文件的内容标识,以及一个请求软件许可的信息;

在中心点,根据从终端用户处接收到的存储媒介标识和内容标识,通过一个签名生成过程,用一个由中心点管理的检验关键码生成一个第一检验代码;

在中心点通过用一个用户关键码对检验关键码加密,生成一个加密的检验关键码;

将第一检验代码和加密的检验关键码从中心点发往终端用户处;

在终端用户处,将从中心点收到的第一检验代码和加密的检验关键码写入目标存储媒介中;

在终端用户处,通过借助用户关键码对储存在目标存储媒介中的加密检验关键码解密,获得一个解密的检验关键码;

在终端用户处,为验证的目的,使用解密的检验关键码,对存

储媒介标识和内容标识采用一个签名生成处理，生成一个第二检验代码；

比较储存在目标存储媒介中的第一检验代码和在终端用户端生成的第二检验代码；和

如果第一和第二检验代码相互一致，则读出储存在主存储媒介中的主题数据文件，并将其写入目标存储媒介。

4. 一个软件复制系统，用于在合法状态下，通过在请求许可复制软件的终端用户和管理许可的中心点之间的通信，将记录在主存储媒介中的软件复制到目标存储媒介中去，软件复制系统包括：

内容标识读取设备，读取唯一分配给一个软件产品的第一标识，该标识和软件都记录在主存储媒介中；

存储媒介标识读取设备，读取记录在目标存储媒介中并唯一分配给目标存储媒体的第二标识；

变换关键码生成设备，设在中心点，根据所述内容标识读取设备读取的第一标识生成一个存储媒介变换关键码，根据所述存储媒介标识读取设备读取的第二标识生成一个主媒介变换关键码，并用第二标识分别对存储媒介变换关键码和主媒介变换关键码加密，生成一个加密的存储媒介变换关键码和一个加密的主媒介变换关键码；

变换关键码写入设备，将所述变换关键码生成设备生成的加密的存储媒介变换关键码写入目标存储媒介；

变换关键码解密设备，用所述存储媒介标识读取设备读出的第二标识，分别对所述变换关键码生成设备生成的加密存储媒介变换关键码和加密主媒介变换关键码解密，生成一个解密的存储媒介变换关键码和一个解密的主媒介变换关键码；

数据解密设备，读出记录在主存储媒介中的目标数据文件并通过用所述变换关键码解密设备生成的解密主媒介变换关键码，对目标数据文件解密，产生一个明文数据文件；

数据写入设备，用所述变换关键码解密设备生成的已解密存储媒介变换关键码对明文数据文件加密，生成一个加密数据文件，并

将加密数据文件写入目标存储媒介。

5. 依据权利要求 4 的软件复制系统，其中所述的变换关键码生成设备包括：

第一加密设备，用一个由中心点管理的主关键码，对所述内容标识读取设备读出的第一标识加密，生成存储媒介变换关键码；

第二加密设备，用主关键码对所述存储媒介标识读取设备读出的第二标识加密，产生主媒介变换关键码；

第三加密设备，用所述存储媒介标识读取设备读出的第二标识，对存储媒介变换关键码和主媒介变换关键码加密，产生加密的存储媒介变换关键码和加密的主媒介变换关键码。

6. 一个软件复制方法，用于将记录在主存储媒介中的主题数据文件复制到目标存储媒介中，其中用主媒介变换关键码对主题数据文件加密，该主媒介变换关键码是根据标识软件产品的内容标识和发放软件产品复制许可的中心点所管理的主关键码而产生的，该软件复制方法包括步骤：

从终端用户处向中心点发送一个唯一分配给主题数据文件的内容标识和一个唯一分配给目标存储媒介的存储媒介标识；

在中心点，用一个由中心点管理的主关键码，分别对内容标识和存储媒介标识加密，产生一个主媒介变换关键码和一个存储媒介变换关键码；

用存储媒介标识，分别对存储媒介变换关键码和主媒介变换关键码加密，生成一个加密的存储媒介变换关键码和一个加密的主媒介变换关键码；

从中心点向终端用户处发送加密的主媒介变换关键码和加密的存储媒介变换关键码；

把加密存储媒介变换关键码写入目标存储媒介；

用存储媒介标识，分别对加密的存储媒介变换关键码和加密的主媒介变换关键码解密，生成一个解密的存储媒介变换关键码和一个解密的主媒介变换关键码；

通过用解密的主媒介变换关键码对目标数据文件解密，将记录

在主存储媒介中的主题数据文件解密，而产生一个明文数据文件；

用解密的存储媒介变换关键码对明文数据文件加密，生成一个加密的数据文件；

将加密的数据文件写入目标存储媒介中。

软件复制系统和方法

技术领域

本发明涉及软件复制系统，尤其是一种可以在合法情况下把享有版权的软件复制到用户的存储媒体上的软件复制系统。

背景技术

近年来，人们采用了许多种软件销售方法，消费者能够购买到储存在某些存储媒体如软盘、高密度光盘只读存储器（CD－ROM）和半导体存储器中的软件产品。它们还能通过网络下载买到联机商店中出售的某些软件产品。然而，大多数商业软件产品可以很简单地被复制到其它存储媒体上。这意味着它们面临着潜在的被非法复制或软件侵权的危险，对享有版权的软件来说，这已经成为一个严重的问题。

在对计算机应用软件、词典、音频和视频数据等的软件销售方法中，一个常用的方法是在一个用保护关键字进行电子加锁的 CD－ROM 中销售软件。当一个用户对某个软件产品发生兴趣时，他/她与经营该产品的一个中心点取得联系。然后用户通过一个必要的过程购买产品，接着得到一个属于该产品的关键字。用这个关键字打开被保护的软件文档，用户最终便能够将软件安装到他/她的系统中了。

销售软件的另一种方法是使用一种含有一些事先生成的特别许可标识信息的可写存储媒体，在中心点对这种信息进行管理以授权复制软件产品。当试图复制记录在 CD－ROM 中的软件产品时，用户或销售存储媒体的零售商将向中心点发生请求。在随后的一些必要的购买该主题软件产品的过程之后，发出请求的用户或零售商收到由中心点发出的标识信息。只有在所收到的标识信息与已经记录在存储媒体（CD－ROM）上的特别许可标识信息相符时，才能从 CD－ROM 向存储媒体复制该主题软件产品。

但是，一旦软件已安装在他/她本地的存储装置如硬盘上时，任何人都能运行或访问软件。这显示意味着，由于缺少关键字保护，已安装的软件仍然有非法复制的问题。

而且，在上述第二种方法中，中心点应与制造存储媒体的工厂保持密切的联系，控制与许可相关的标识信息。存储媒体的另一个问题是，需要根据两个不同目的，用不同的方式处理两种类型的存储媒体：软件复制与一般使用。

欧洲专利 No.0302710A2 公开了一种在软件运行时对软件进行版权保护的方法。在磁盘上分布的 PC 软件的版权保护通过以下方式实现：提供存储在 PC 的 ROM 中的一个唯一标识（ID），而磁盘上的软件就要在该 ROM 中使用。这个 ID 可由 PC 的用户访问。想要保护通过磁盘分发的软件不被非法复制的提供商在分发的磁盘上使用任何可用的加密方式提供一个源 ID，以产生编码的检验字。该检验字被生成。在安装期间被写入分发的磁盘上并复制到由该用户的个人计算机进行的所有备

份版本上。在每次使用该程序前，磁盘上的软件使用PC和源ID以及检验字来验证是否在其被安装的那台PC上使用该软件。换言之，现有技术提供了一种在软件被运行时对其进行版权保护的方法，但是没有可在将软件程序写入目标介质时提供版权保护的技术。

发明内容

考虑到上面所述的问题，本发明的目标是提供一种软件复制系统，该系统可以使记录在主记录介质上的受版权保护的数据以合法的方式被复制到用户可以读、写的目标存储介质上。即，本发明可以实现在将软件程序写入目标存储介质时进行软件保护的效果。

为了实现上述目标，依据本发明，提供了一个软件复制系统，在合法情况下，将记录在一个主存储媒体上的软件复制到一个目标存储媒体上。通过请求许可复制软件产品的终端用户和管理许可的中心点间的通信，完成一个授权的复制过程。

该软件复制系统包括下列组成部件。内容标识读取装置，从主存储媒体中读出第一标识。这个第一标识唯一地分配给记录在主存储媒体上的软件产品。存储媒体标识读取装置，从目标存储媒体中读出第二标识。这个第二标识唯一地分配并储存在目标存储媒体中。设在中心点的签名生成装置，由内容标识读取装置读出的第一标识和存储媒体标识读取装置读出的第二标识生成第一签名。这个第一签名作为允许复制软件产品的一个证明。签名写入装置将签名生成装置生成的第一签名写入目标存储媒体。出于验证的目的，签名生成/比较装置根据内容标识读取装置读出的第一标识和存储体标识读取装置读出的第二标识生成第二签名。然后，签名生成/比较装置将存储在目标存储媒体中的第一签名与该第二签名进行比较。当签名生成/比较装置所作的比较结果证实第一和第二标识相同时，数据复制装置从主存储媒体中检索出软件产品并将其写入目标存储媒体。

为了达到上述目的，还提供了一个软件复制方法，在合法状态下，将记录在主存储媒体上的软件复制到目标存储媒体上。这个软件复制方法包括下面的步骤。

第一，从终端用户向中心点发出一个唯一分配给目标存储媒体的存储媒体标识和一个唯一分配给主题数据文件的内容标识，以及一个软件许可的请求信息。第二，在中心点，根据从终端用户处收到的存储媒体标识和内容标识生成一个第一检验代码。这一步骤通过用中心点管理的检验关键字执行签名生成过程而完成。第三，在中心点用一个用户关键字对检验关键字加密，生成一个加密的检验关键字。第四，从中心点向终端用户发送第一检验代码和加密的检验关键字。第五，从中心点到达终端用户的第一检验代码和加密的检验关键字被写入目标存储媒体。第六，在用户终端，借助用户关键字对储存在目标存储媒体中的加密的检验关键字进行解密，得到一个已解密的检验关键字。第七，出于在终端用户处进行验证的目的，用已解密的检验关键字对存储媒体标识和内容标识实施一个签名生成过程，生成一个第二检验代码。第八，用储存在目标存储媒体中的第一检验代码与在终端用户处生成的第

二检验代码进行比较。最后，如果第一和第二检验代码相互一致，则储存在主存储媒体中的主题数据文件被读出并写入目标存储媒体。

本发明还提供一个软件复制系统，用于在合法状态下，通过在请求许可复制软件的终端用户和管理许可的中心点之间的通信，将记录在主存储媒介中的软件复制到目标存储媒介中去，软件复制系统包括：内容标识读取设备，读取唯一分配给一个软件产品的第一标识，该标识和软件都记录在主存储媒介中；存储媒介标识读取设备，读取记录在目标存储媒介中并唯一分配给目标存储媒体的第二标识；变换关键码生成设备，设在中心点，根据所述内容标识读取设备读取的第一标识生成一个存储媒介变换关键码，根据所述存储媒介标识读取设备读取的第二标识生成一个主媒介变换关键码，并用第二标识分别对存储媒介变换关键码和主媒介变换关键码加密，生成一个加密的存储媒介变换关键码和一个加密的主媒介变换关键码；变换关键码写入设备，将所述变换关键码生成设备生成的加密的存储媒介变换关键码写入目标存储媒介；变换关键码解密设备，用所述存储媒介标识读取设备读出的第二标识，分别对所述变换关键码生成设备生成的加密存储媒介变换关键码和加密主媒介变换关键码解密，生成一个解密的存储媒介变换关键码和一个解密的主媒介变换关键码；数据解密设备，读出记录在主存储媒介中的目标数据文件并通过用所述变换关键码解密设备生成的解密主媒介变换关键码，对目标数据文件解密，产生一个明文数据文件；数据写入设备，用所述变换关键码解密设备生成的已解密存储媒介变换关键码对明文数据文件加密，生成一个加密数据文件，并将加密数据文件写入目标存储媒介。

本发明还提供一个软件复制方法，用于将记录在主存储媒介中的主题数据文件复制到目标存储媒介中，其中用主媒介变换关键码对主题数据文件加密，该主媒介变换关键码是根据标识软件产品的内容标识和发放软件产品复制许可的中心点所管理的主关键码而产生的，该软件复制方法包括步骤：从终端用户处向中心点发送一个唯一分配给主题数据文件的内容标识和一个唯一分配给目标存储媒介的存储媒介标识；在中心点，用一个由中心点管理的主关键码，分别对内容标识和存储媒介标识加密，产生一个主媒介变换关键码和一个存储媒介变换关键码；用存储媒介标识，分别对存储媒介变换关键码和主媒介变换关键码加密，生成一个加密的存储媒介变换关键码和一个加密的主媒介变换关键码；从中心点向终端用户处发送加密的主媒介变换关键码和加密的存储媒介变换关键码；把加密存储媒介变换关键码写入目标存储媒介；用存储媒介标识，分别对加密的存储媒介变换关键码和加密的主媒介变换关键码解密，生成一个解密的存储媒介变换关键码和一个解密的主媒介变换关键码；通过用解密的主媒介变换关键码对目标数据文件解密，将记录在主存储媒介中的主题数据文件解密，而产生一个明文数据文件；用解密的存储媒介变换关键码对明文数据文件加密，生成一个加密的数据文件；将加密的数据文件写入目标存储媒介中。

下面结合描述本发明最佳实施方案示例的附图和叙述，本发明上述及其他目标、特性和优点将更为清晰。

附图说明

图1是依据本发明的软件复制系统的概念性视图;

图2显示在本发明第一实施方案中软件复制系统进行的软件复制过程的流程图;

图3（A）是CD－ROM结构的示意图;

图3（B）是MO盘片结构的示意图;

图4是显示复制版权软件过程的示意图;

图5是一个典型的签名处理器的结构的示意图;

图6是显示执行复制的软件程序的过程的示意图;

图7显示在本发明第二实施方案中软件复制系统执行的软件复制过程的流程图;

图8是在中心点的处理过程示意图;

图9是终端用户处理过程的示意图;

图10是执行复制的软件程序的过程的示意图.

具体实施方式

在开始部分，将参照图1对本发明作一个概括描述，图1是依据本发明的软件复制系统的概念性视图。

如在图1中所见到的，本发明的软件复制系统包括下述几个部件。内容标识读取装置2是一个用来读出储存在主存储媒体1中的第一标识的装置。这个第一标识唯一地分配给每一个记录在主存储媒体1中的软件产品。存储媒体标识读取装置4读出储存在目标存储媒体3中的第二标识。这个第二标识唯一地分配给目标存储媒体3。签名生成装置6，设在管理软件复制许可的一个中心点5，根据分别由内容标识读取装置2和存储媒体标识读取装置4读出的第一和第二标识生成第一签名。第一签名作为许可复制软件产品的证明。签名写入装置7把签名生成装置6生成的第一签名写入目标存储媒体3。签名生成/比较装置8根据分别由内容标识读取装置2和存储媒体读取装置4读出的第一和第二标识产生第二签名。签名生成/比较装置8比较储存在目标存储媒体3中的第一签名和产生的第二签名。当签名生成/比较装置8进行比较的结果证实第一和第二签名是相同的时，数据复制装置9从主存储媒体中检索出主题软件产品并将其写入目标存储媒体3.

主存储媒体1包含若干商业软件产品，每个上都写有一个内容标识。目标存储媒体3有一个单独的存储媒体标识，这个标识在工厂发货之前就已写入。当一个用户从主存储媒体1中选择了一个软件产品时，内容标识读取装置2检索一个与所选软件产品相对应的内容标识，然后存储媒体标识读取装置4读出记录在目标存储媒体3中的存储媒体标识。这两个标识与购买订单信息一起被发往中心点5，以请求许可复制主题软件产品。在中心点5，签名生成装置6接收内容标识和存储媒体标识，并向用户返回一个根据收到的标识而生成的签名。这个签名向用户授予了许可复制软件产品的权利。同时，随着发放签名，在中心点5的一个用户情况数据库中登记用户，并进行记帐处理。

在用户端，接收到从签名生成装置6发出的签名后，签名写入

装置7将其写入目标存储媒体3。接着，签名生成/比较装置8在本地根据内容标识读取装置2检索到的内容标识和存储媒体标识读取装置4检索到存储媒体标识生成一个签名。签名生成/比较装置8对这个签名和储存在目标存储媒体3中的第一次提到的签名作比较。如果两个签名相互一致，则数据复制装置9从主存储媒体1中检索出以加密形式储存的主题软件产品，并将其复制到目标存储媒体3中。但是，现在储存在目标存储媒体3中的软件并不能运行，因为它还是加密的。用户必须将它加载到一个特殊处理器的主存储器上，该处理器对加密的软件进行解码并运行。

下面，参照图2至6对本发明的第一实施方案进行描述。下面的解释假设这样一种情况，即某一享有版权在CD-ROM中销售的软件程序将被复制到一张磁光(MO)盘片上。

图2是软件复制系统执行的软件复制过程的流程图。为了使用本发明的软件复制系统将一个CD-ROM中的程序复制到一张MO盘片上，需要下列步骤：

[S1] 记录在MO盘片上的存储媒体标识*IDk*和主题软件程序的软件标识*SIDi*被发往管理软件复制许可的中心点。

[S2] 在中心点处理这个软件许可请求，根据从终端用户处收到的存储媒体标识*IDk*和软件标识*SIDi*生成一个检验代码*CS*。然后，中心点将检验代码*CS*返回给终端用户。

[S3] 到达终端用户处的检验代码*CS*被写入MO盘片中一个预定的存储区。

[S4] 出于验证的目的，在终端用户基于发送到中心点的存储媒体标识*IDk*和软件标识*SIDi*本地生成另一个检验代码*CS'*。

[S5] 本地生成的检验代码*CS'*与储存在MO盘片中的另一检验代码*CS*进行比较。

[S6] 根据*CS*和*CS'*比较的结果，以不同的方式进行处理。如果发现两个检验代码相同，处理过程进行到下一个步骤S7。否则，处理过程不从CD-ROM向MO盘片复制软件程序而被终止。

[S7] 将一个有软件标识*SIDi*的加密软件数据文件从

CD-ROM复制到准备好的MO盘片上。

图3(A)和3(B)分别显示了CD-ROM和MO盘片中记录的结构。CD-ROM11的结构如图3(A)所示，记录了多个版权软件程序和一个管理应用程序MA。以加密形式储存的版权软件程序有它们各自的软件标识 *SIDi*(I=1, 2, ..., n)。管理应用程序 *MA* 控制从CD-ROM向MO盘片复制版权软件程序的操作。针对软件复制请求，这个程序将被加载并在一个位于终端用户处的终端站上运行（如一台个人计算机）。也就是，管理应用程序 *MA* 负责图2所示的过程中在终端用户处运行的那部分步骤。

图3(B)是一个显示MO盘片12记录结构的示意图，在MO盘片上记录了一个存储媒体标识 *IDk*(k=1, 2, ..., m)。虽然用户可以对MO盘片12的大部分区域自由地写与/或读，但存储媒体标识 *IDk* 被写在盘片上一个特定的不能重写的部位。这个存储媒体标识 *IDk* 可以是一个序列号，发货前在工厂中唯一分配给每个媒体。

下面的叙述参照图4，将展示一个更为详细的从CD-ROM向MO盘片复制版权软件过程。

图4显示了一个软件复制过程，它大致分为两个部分：在终端用户方的步骤（图4的右半部分）和在中心点的步骤（图4的左半部分）。在终端用户方，一个终端站（如一台个人计算机）执行有关软件复制的实际数据处理工作，而在中心点的若干设备则管理软件复制的许可。两处通过一条通信线路或一个传递信道相互连接。

终端用户处的终端站配有一个CD-ROM驱动器和一个MO驱动器（图中均未显示）。作为储存版权软件程序的主存储媒体的CD-ROM11被插入CD-ROM驱动器。另一方面，作为目标存储媒体的MO盘片12被装入MO驱动器。CD-ROM11中的主题软件程序有一个软件标识 *SIDi*，而MO盘片12则具有唯一的存储媒体标识 *IDk*。

首先，在终端用户的终端站，CD-ROM11中的管理应用程序 *MA* 从终端用户接收一个复制特定软件程序的请求。针对这个请求，管理应用程序 *MA* 从CD-ROM11中读出相应的软件标识 *SIDi*

并从 MO 盘片 12 中提取存储媒体标识 *IDk*。这两个标识与包含软件许可所需信息的请求信息一起被送往软件许可中心。

中心点从用户那里接收上述请求并把请求的内容储存到一个用户情况数据库 13 中。接收到的软件标识 *SIDi* 和存储媒体标识 *IDk* 被提供给签名处理器 14，在那里把标识 *SIDi* 和 *IDk* 压缩为一个检验代码 *CS*。在这个压缩过程中，使用一个检验关键字 *KEYc* 作为个人关键字（或密码）。产生的检验代码 *CS* 作为图 1 中所称的“签名”使用。被签名处理器 14 使用的检验关键字 *KEYc* 被直接送到加密单元 15，在那里用一个用户关键字 *KU* 对其进行加密，产生一个密文 *EKU(KEYc)*。签名处理器 14 生成的检验代码 *CS* 和加密单元 15 生成的密文 *EKU(KEYc)* 最后与中心点标识 *IDc* 一起被送到终端用户处，作为终端用户所发请求的响应。

在终端用户端，终端站从中心点接收信息，从中提取检验代码 *CS* 和密文 *EKU(KEYc)*，并将其写入目标 MO 盘片 12 中。记录在 MO 盘片 12 上的检验代码 *CS* 和密文 *EKU(KEYc)* 被检索出来并送到管理应用程序。

接着，在终端站，开始进行一个签名验证处理。首先，解密单元 16 借助用户关键字 *KU* 对密文 *EKU(KEYc)* 解码，并提取曾在中心点加密的检验关键字 *KEYc*，根据 CD-ROM11 提取的软件标识 *SIDi* 和从 MO 盘片 12 中提取的存储媒体标识 *IDk*，为在用户终端进行验证，签名处理器 17 生成一个检验代码 *CS'*。由解密单元 16 解密的检验关键字 *KEYc* 在这个 *CS'* 生成过程中使用。然后，比较器 18 对写在 MO 盘片 12 中的检验代码 *CS* 和由签名处理器 17 生成的检验代码 *CS'* 进行比较。如果比较结果说明 *CS* 和 *CS'* 两个代码是一致的，开关 19 将允许具有软件标识 *SIDi* 的软件程序以加密数据形式被写入到目标 MO 盘片 12 中去。

下面的叙述将说明一个由中心点的签名处理器 14 和终端用户端的签名处理器 17 实现的典型功能。

图 5 描述了包括一个异或逻辑单元 21 和一个加密单元 22 的签名处理器。异或逻辑单元 21 在软件标识 *SIDi*、存储媒体标识 *IDk*

和检验代码 *CS* 上执行一个异或操作。加密单元 22 用检验关键字 *KEYc* 对异或逻辑单元 21 的输出加密，以产生检验代码 *CS*。这两个单元 21 和 22 构成一个散列函数操作器。

在逐块方式下，加密单元 22 用检验关键字 *KEYc* 对软件标识 *SIDi* 和存储媒体标识 *IDk* 加密。加密的输出数据被反馈回异或逻辑单元 21 的输入端，并与下一个数据块一起进行异或逻辑运算。异或逻辑电路 21 的输出又被加密单元 22 再一次进行加密。上述操作不断重复，直到最后一个块进入，当最后一个模块的加密完成后，这个循环计算的结果将作为一个检验代码 *CS* 从加密单元 22 输出。

经过许可的软件程序以上述方式复制到 MO 盘片 12 中，但终端用户不能运行它，因为程序还是加密的。下面的叙述会解释如何使其可以运行。

图 6 显示了一个执行复制的软件程序的过程。MO 盘片 12 包含检验代码 *CS*、密文 *EKU(KEYc)*、存储媒体标识 *IDk* 和软件标识 *SIDi* 及以加密数据 *EKd(DATA)*形式储存的复制软件。这种加密数据 *EKd(DATA)*在软件刻到 CD-ROM 上之前被用关键字 *Kd* 作了加密处理，而加密关键字 *Kd* 在管理应用程序的管理之下。

终端用户的终端站首先从 MO 盘片 12 中检索出检验代码 *CS*、密文 *EKU(KEYc)*、存储媒体标识 *IDk* 和软件标识 *SIDi*。解密单元 16 借助用户关键字 *Ku* 对密文 *EKU(KEYc)*解密，从而提取出检验关键字 *KEYc*。随后，签名处理器 17 用经过解密单元 16 解密的检验关键字 *KEYc*，根据从 MO 盘片 12 接收到的软件标识 *SIDi* 和存储媒体标识 *IDk* 生成另一个检验代码 *CS′*。尔后，比较器 18 比较检验代码 *CS* 和 *CS′*。如果比较说明两个代码 *CS* 和 *CS′*是一致的，开关 19 将允许一个包含加密软件程序的加密数据文件 *EKd(DATA)*通过，送入解密单元 25。解密单元 25 用管理应用程序拥有的关键字 *Kd* 对加密的数据文件 *EKd(DATA)*解密，恢复原来的明文（未加密）数据文件 *DATA*。这个解密的数据文件 *DATA* 的内容可以由中央处理单元(CPU)在加载到存储器中后运行，CPU 和

存储器都是终端站中 CPU/存储器单元 26 的一部分。

下面，参照图 7 到 10 描述本发明的第二实施方案。在第二实施方案中，每个记录在 CD-ROM 中的软件程序有一个唯一分配的软件标识 *DID*，它对应的数据文件 *Data* 储存为一个加密数据文件 *EKa(Data)*。这个加密数据文件 *EKa(Data)*是用根据在软件许可中心管理的软件标识 *DID* 和主关键字 *KM* 生成的主媒体变换关键字 *Ka* 来生成的。软件许可中心负责他们的商业软件产品复制权的许可工作。至于目标存储媒体，用户的 MO 盘片有一序列号，用作存储媒体标识 *Mid*。

图 7 是在上述假设下，第二实施方案的软件复制系统执行软件复制过程的流程图。

为了获得在 CD-ROM 中销售的软件程序的复本，必须经过以下 7 个步骤：

[S11] 目标 MO 盘片中记录的存储媒体标识 *Mid* 和 CD-ROM 中的主题软件程序的软件标识 DID 被从终端用户传送到控制复制软件产品许可的软件许可中心。

[S12] 在软件许可中心，测试软件标识 *DID* 是否登记过。

[S13] 用在软件许可中心管理的主关键字 *KM* 对存储媒体标识 *Mid* 和软件标识 *DID* 加密，分别生成一个存储媒体变换关键字 *Ku* 和主媒体变换关键字 *Ka*。

[S14] 通过用存储媒体标识 *Mid* 对存储媒体和主媒体变换关键字 *Ku* 和 *Ka* 加密，生成一个密文 *EMid(Ku, Ka)*。密文 *EMid(Ku, Ka)*被送到终端用户方，作为请求的响应信息。

[S15] 储存密文 *EMid(Ku)*，即密文 *EMid(Ku, Ka)*中与 MO 盘片相关的部分，而不试图解密，同时，终端用户通过用存储媒体标识 *Mid* 对接收到的密文 *EMid(Ku, Ka)*解密，获得存储媒体变换关键字 *Ku* 和主媒体变换关键字 *Ka*。

[S16] 用步骤 S15 中得到的主媒体变换关键字 *Ka*，对 CD-ROM 中对应于软件标识 *DID* 的加密数据文件 *EKa(Data)*解密，恢复原来的明文数据文件 *Data*。

[S17] 用步骤15得到的存储媒体变换关键字*Ku*对明文数据文件*Data*再次加密，加密数据文件储存到MO盘片中，这样就结束了软件复制过程。

下面将对上述软件复制过程作更详细的讨论。在本发明的第二实施方案中，过程从在终端用户端向软件许可中心发送请求开始，作为过程的一部分，这只包含下面两个内容。一个是读出目标MO盘片的存储媒体标识*Mid*和储存在CD-ROM中的主题软件的软件标识*DID*，另一个是向软件许可中心发送标识*Mid*和*DID*。下面的叙述省略了这两个步骤，而从软件许可中心接收到从终端用户来的上述请求后所执行的步骤开始。

图8解释了在软件许可中心执行的过程。通过一条通信线路从终端用户那里接收到两个标识*Mid*和*DID*后，软件许可中心把存储媒体标识*Mid*转给具有中心控制的主关键字*KM*的加密单元31，并将软件标识*DID*提供给比较器32。加密单元31用主关键字*KM*对存储媒体标识*Mid*加密，生成一个存储媒体变换关键字*Ku*。另一方面，比较器32寻找一个内容标识文件33，对每个条目和接收到的软件标识*DID*作比较，来验证其有效性。如果接收到的软件标识*DID*与内容标识文件33中登记的一个条目一致，比较器32关闭开关34，从而允许软件标识*DID*进入具有主关键字*KM*的加密单元35。加密单元35用主关键字*KM*对软件标识*DID*加密，生成一个主存储媒体变换关键字*Ka*。加密单元31生成的存储媒体变换关键字*Ku*和加密单元35生成的主存储媒体变换关键字*Ka*被输入到加密单元36，用存储媒体标识*Mid*作进一步加密。加密单元36生成的密文*EMid(Ku, Ka)*通过通信线路被送往发出请求的终端用户。在上述处理步骤完成时，付帐请求被记入用户概要情况数据库37，费用由发出请求的终端用户承担。

图9解释在上述软件许可中心的处理完成后，终端用户执行的过程。从软件许可中心接收到的密文*EMid(Ku, Ka)*被引入解密单元51，而密文*EMid(Ku)*作为接收密文*EMid(Ku, Ka)*的一部分，被写入目标MO盘片40中一个预定的区域41。解密单元51用从MO

盘片 40 中提取的存储媒体标识 *Mid* 对密文 *EMid(Ku, Ka)*解密，从而恢复原来的存储媒体变换关键字 *Ku* 和主媒体变换关键字 *Ka*。恢复的主媒体变换关键字 *Ka* 再被输入解密单元 52，作为一个解密关键字，而恢复的存储媒体变换关键字 *Ku* 输入加密单元 53，作为它的加密关键字。解密单元 52 在 CD-ROM60 中检索与软件标识 DID 相应的加密数据文件 EKa(Data)，并用主媒体转换关键字 Ka 对其进行解释，于是恢复了原始的明文数据文件 Data。这个数据文件 *Data* 被加密单元 53 用存储媒体变换关键字 *Ku* 再次加密，作为结果的密文 *EKu(Data)*被写入目标 MO 盘片 40。

在上面所述的方法中，用从记录在 MO 盘片 40 中的唯一标识和在软件许可中心控制下的主关键字中获得的两个变换关键字进行处理，将密文 *EKu(Data)*写入 MO 盘片 40。接着在下面描述执行这个加密数据文件 *EKu(Data)*的处理过程。

图 10 描述了执行作为数据文件被复制到 MO 盘片 40 上的软件程序的过程。密文 *EMid(Ku)*被储存在 MO 盘片 40 可重写区域中的一段 41 上，而存储媒体标识 *Mid* 则记录在一个不可重写区域 42 中。加密的数据文件 EKu(Data)储存在其余的可重写区域。为了执行调用加密数据文件 *Eku(Data)*，存储媒体标识 *Mid* 和密文 *EMid(Ku)*被从 MO 盘片 40 中检索出来，并输入一个解密单元 54。解密单元 54 用存储媒体标识 *Mid* 作为解密关键字，对密文 *EMid(Ku)* 解密，以恢复存储媒体变换关键字 *Ku*。另一个解密单元 55 用存储媒体变换关键字 *Ku* 作为解密关键字，对从 MO 盘片 40 中检索出的加密数据文件 *EKu(Data)*解密。所得到的明文数据文件 *Data* 在加载到作为终端用户终端站的个人计算机主存储器中后，将被运行。

将上面所讨论的内容概括如下。依据本发明，软件复制系统包括设在中心点的签名生成装置，用于根据标识目标存储媒体和储存在主媒体中的主题数据的信息生成一个签名。系统还包括，在终端用户方的签名写入装置，用于将签名生成装置生成的签名写入目标存储媒体；签名生成/比较装置，用于对在终端用户本地生成的签

名和已写入目标存储媒体中的签名作比较；数据复制装置，用于根据比较的结果将主题程序复制到目标存储媒体中。因此，中心点只须发放一个与目标存储媒体标识相关的签名，而不必与存储媒体制造工厂保持密切联系来管理任何特别许可信息。这样也就消除了制造商和零售商为了使用存储媒体复制软件而进行的库存控制。

前面的叙述只是对本发明原理的描述。而且，由于本领域技术人员可以很容易地对其作出多种修改和变化，本发明并不仅限于上面所描述和表现的实际设计和应用，因此可以认为所有适当的修改和等价变换都属于本发明所附权利要求及与其相当的范围。

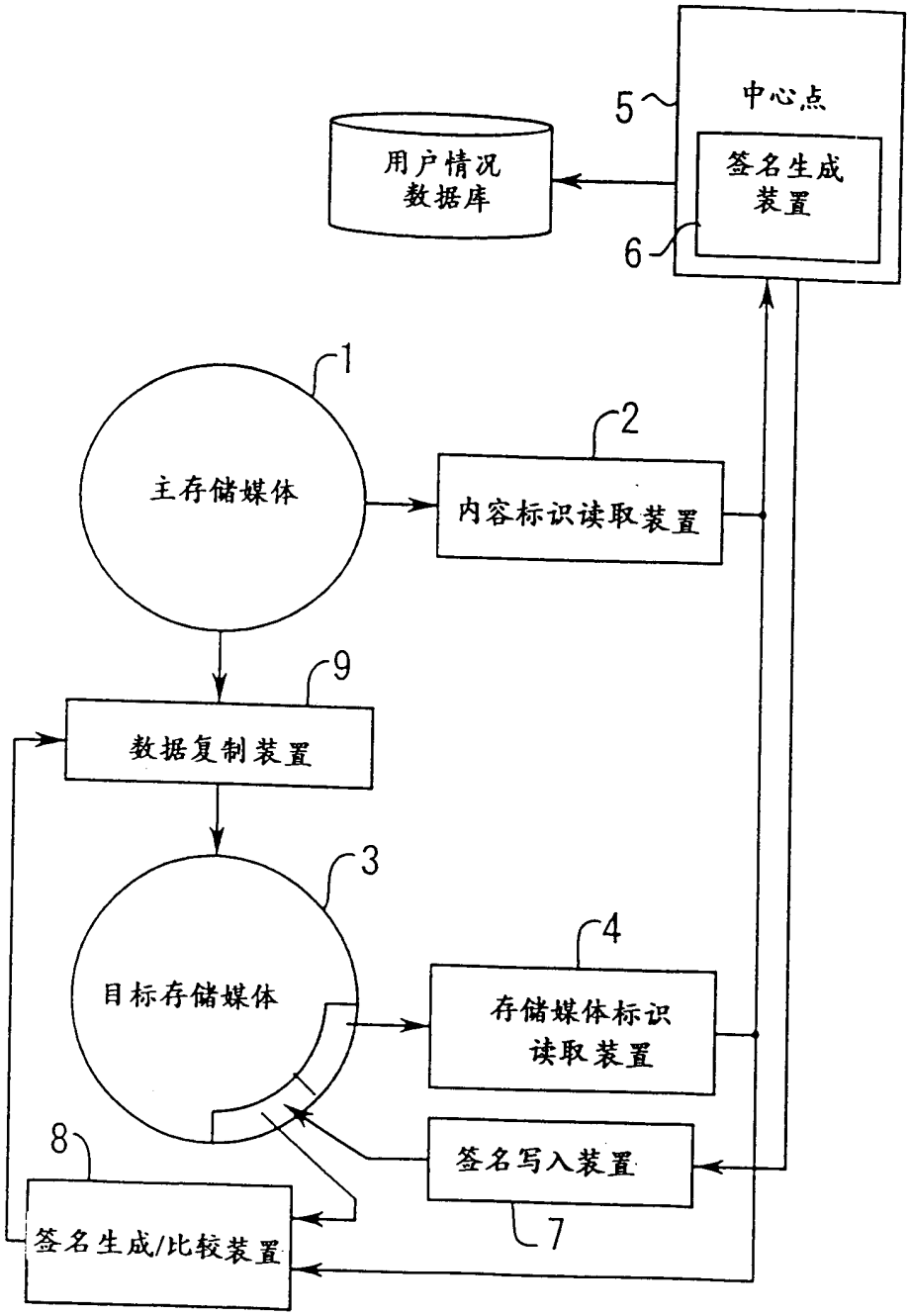

中心点
5
用户情况
数据库
签名生成
装置
6
1
主存储媒体
2
内容标识读取装置
9
数据复制装置
3
目标存储媒体
4
存储媒体标识
读取装置
签名写入装置
7
8
签名生成/比较装置

图 1

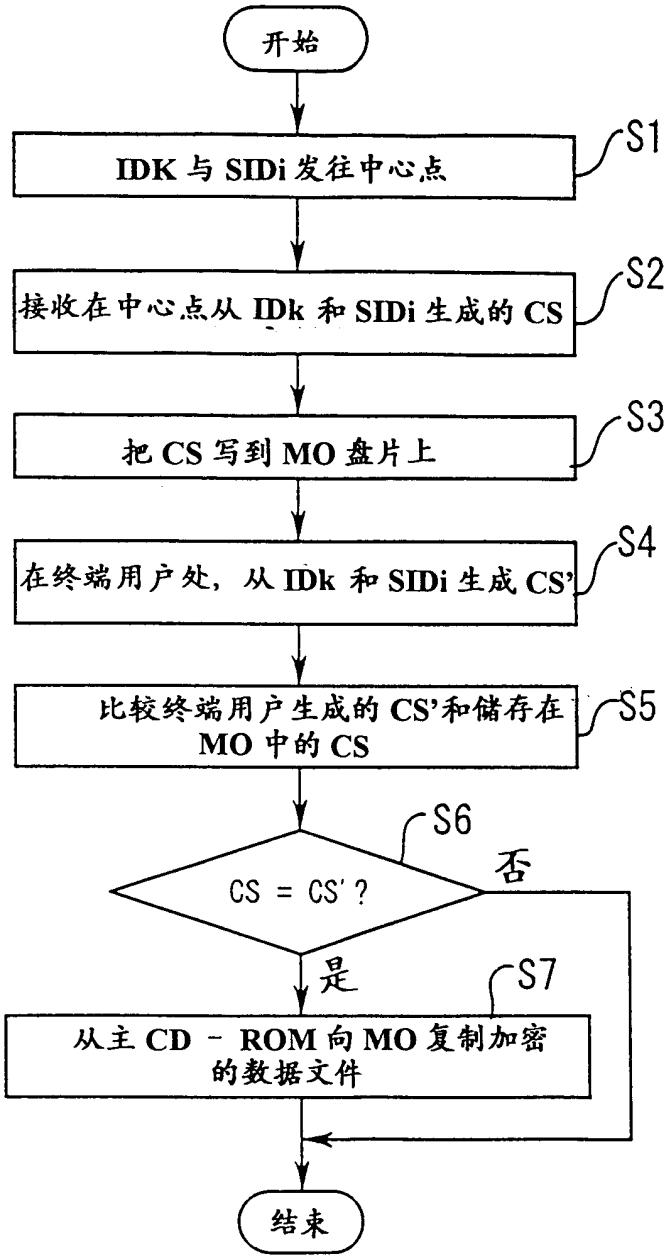

开始
IDK 与 SIDi 发往中心点
S1
接收在中心点从 IDk 和 SIDi 生成的 CS
S2
把 CS 写到 MO 盘片上
S3
在终端用户处，从 IDk 和 SIDi 生成 CS'
S4
比较终端用户生成的 CS'和储存在 MO 中的 CS
S5
S6
CS = CS' ?
否
是
S7
从主 CD - ROM 向 MO 复制加密的数据文件
结束

图 2

图 3 (A)

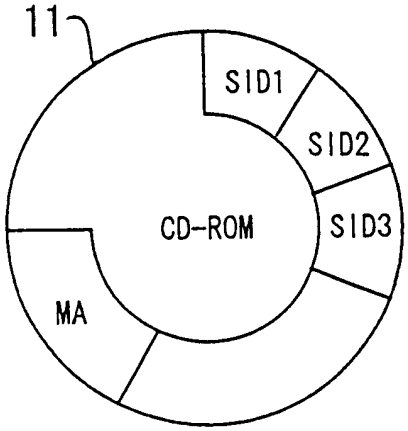
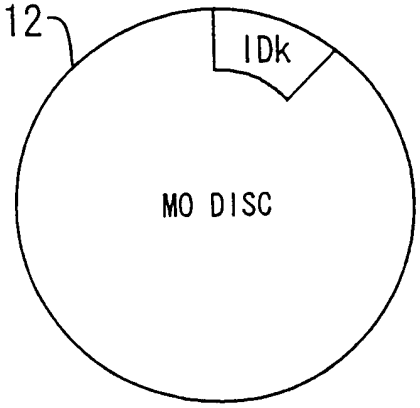


图 3 (B)



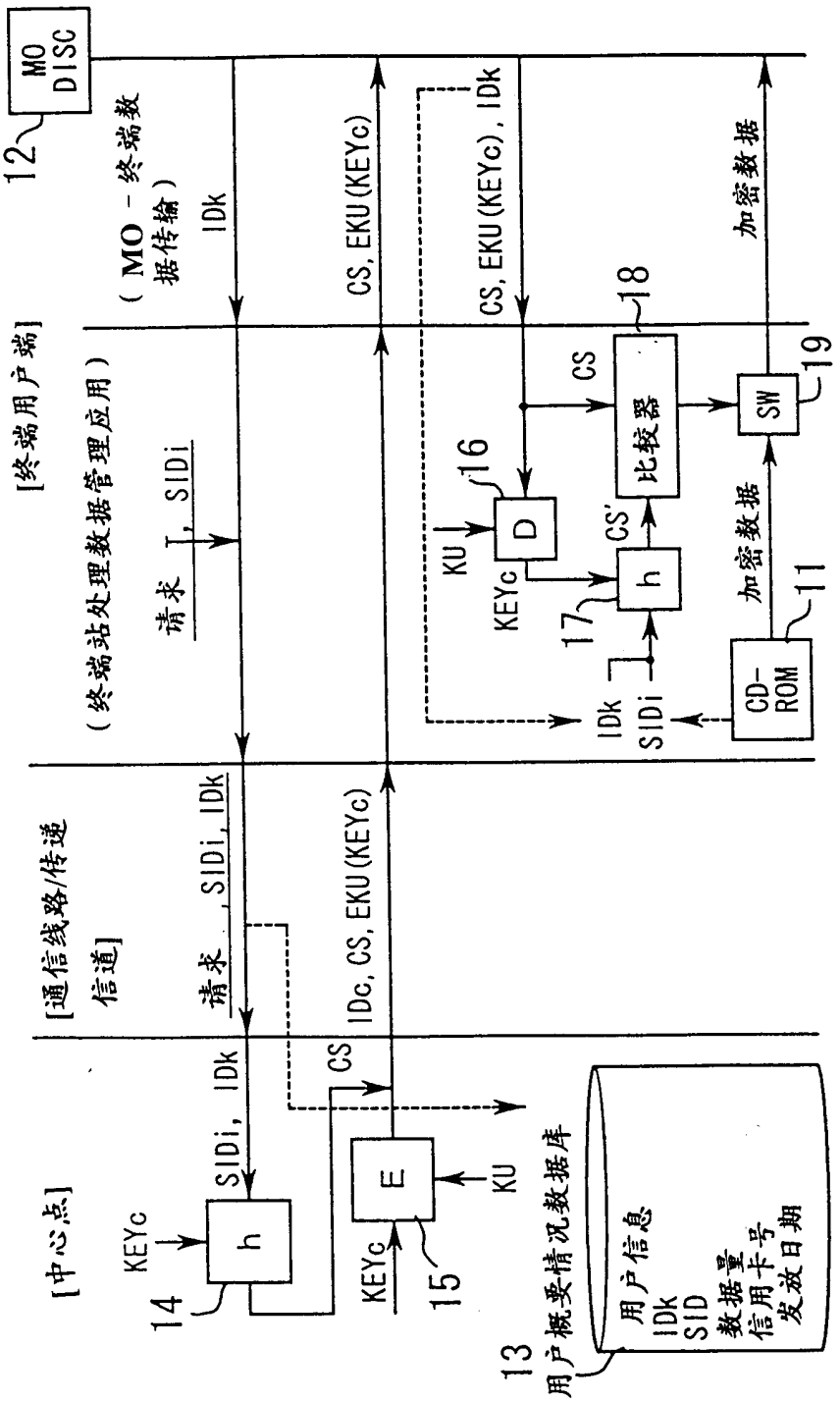

[中心点]
[通信线路/传递信道]
[终端用户端]
(终端站处理数据管理应用)
(MO-终端数据传输)
MO DISC
12
请求 I, SIDi
IDk
CS, EKU(KEYc)
CS, EKU(KEYc), IDk
加密数据
18
CS
比较器
SW
19
16
KU
D
KEYc
17
CS'
h
IDk
SIDi
CD-ROM
加密数据
11
请求 , SIDi, IDk
IDc, CS, EKU(KEYc)
SIDi, IDk
CS
KEYc
14
h
E
15
KU
13
用户概要情况数据库
用户信息
IDk
SID
数据量
信用卡号
发放日期

图 4

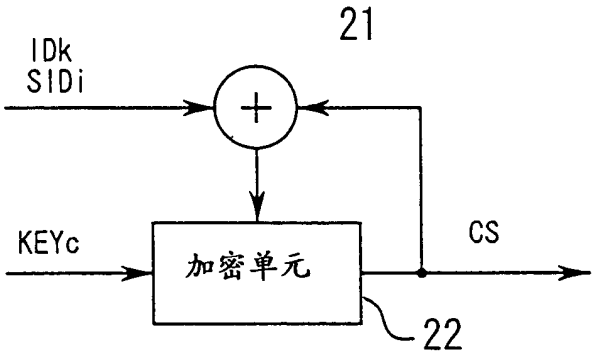


图 5

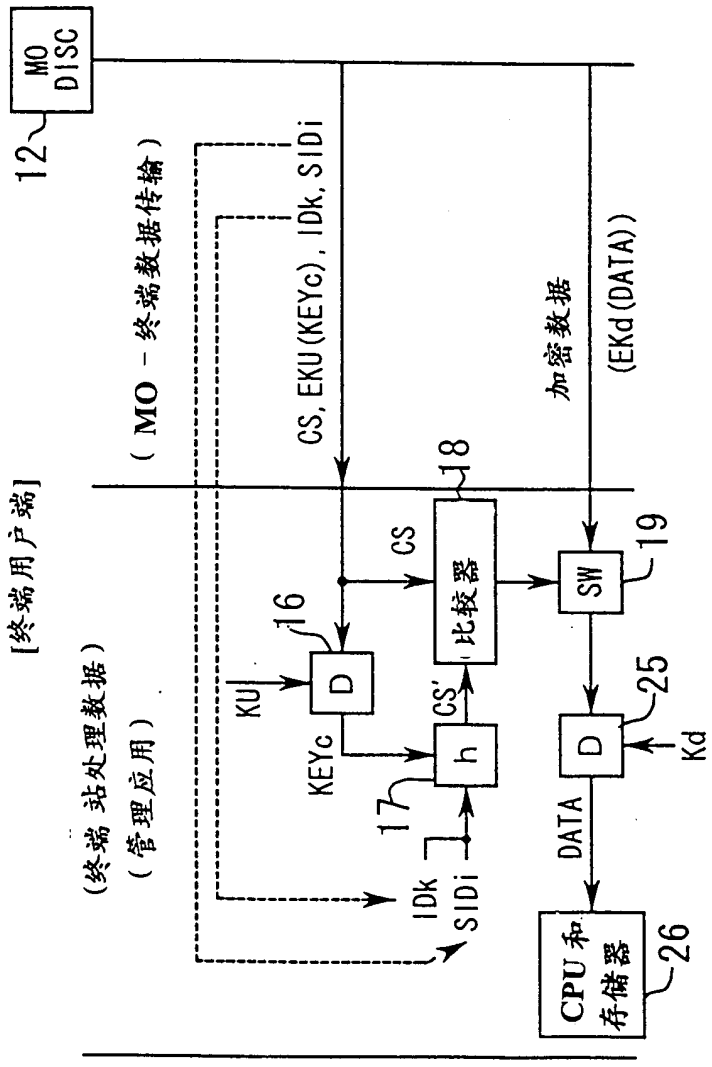

[终端用户端]
(终端 站处理数据)
(管理应用)
MO DISC
12
(MO - 终端数据传输)
CS, EKU(KEYc), IDk, SIDi
加密数据
(EKd(DATA))
18
CS
比较器
SW
19
16
D
KU
KEYc
CS'
h
17
IDk
SIDi
D
25
Kd
DATA
CPU 和 存储器
26

图 6

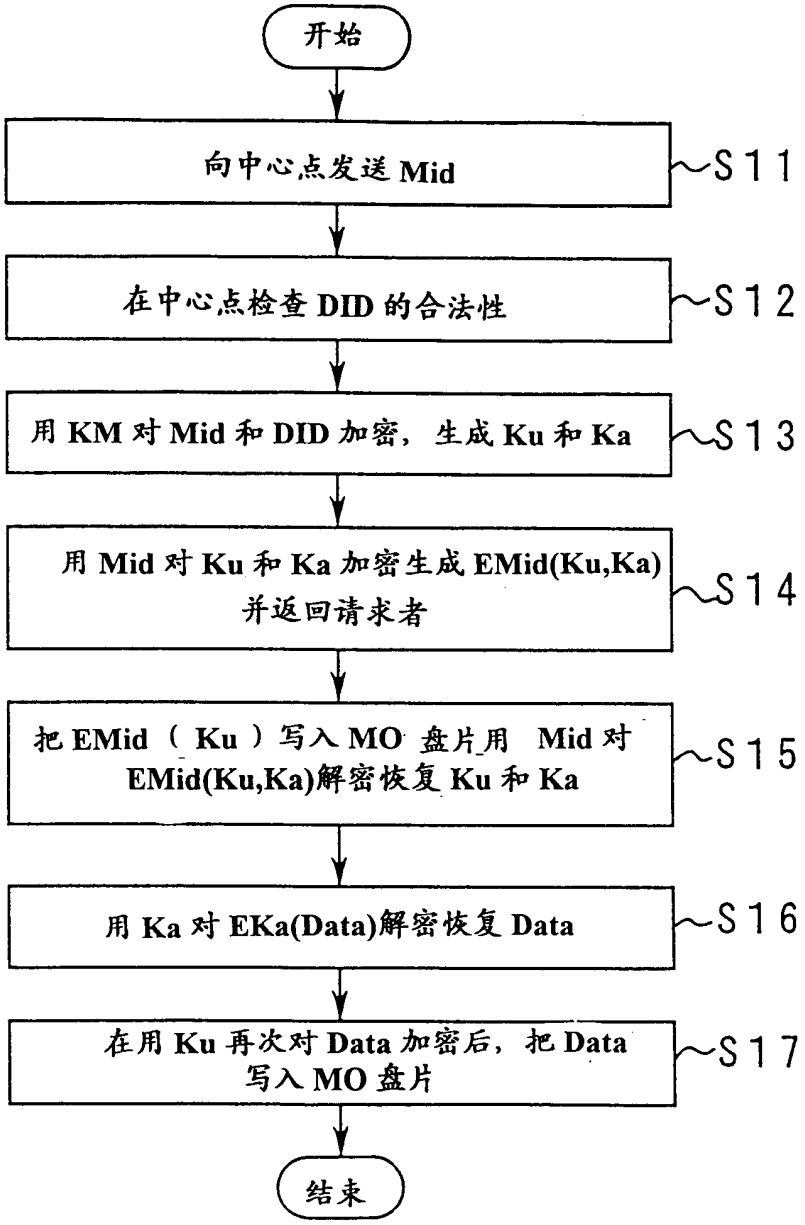

开始
向中心点发送 Mid
S11
在中心点检查 DID 的合法性
S12
用 KM 对 Mid 和 DID 加密，生成 Ku 和 Ka
S13
用 Mid 对 Ku 和 Ka 加密生成 EMid(Ku,Ka)
并返回请求者
S14
把 EMid（ Ku ）写入 MO 盘片用 Mid 对
EMid(Ku,Ka)解密恢复 Ku 和 Ka
S15
用 Ka 对 EKa(Data)解密恢复 Data
S16
在用 Ku 再次对 Data 加密后，把 Data
写入 MO 盘片
S17
结束

图 7

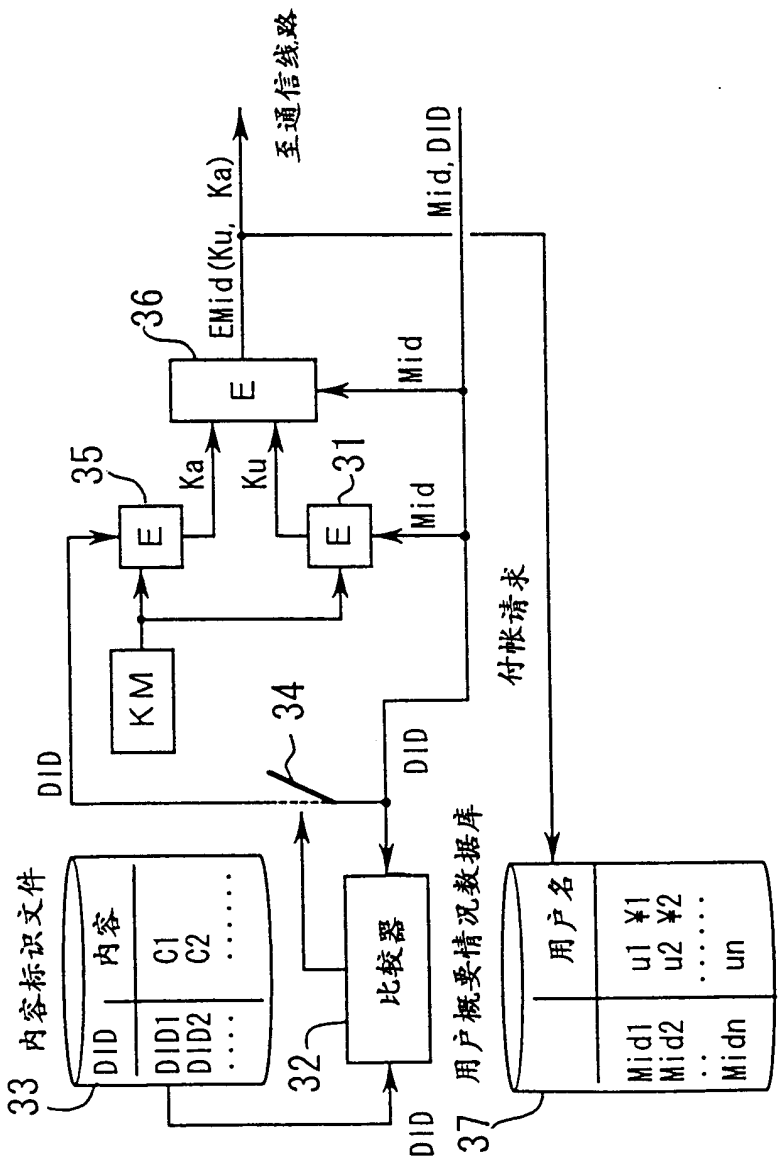

至通信线路
EMid(Ku, Ka)
Mid, DID
36
E
Mid
35
E
Ka
Ku
31
E
Mid
KM
34
DID
DID
付帐请求
内容标识文件
DID
内容
DID1
DID2
C1
C2
33
比较器
32
DID
用户概要情况数据库
用户名
Mid1
Mid2
Midn
u1 ¥1
u2 ¥2
un
37

图 8

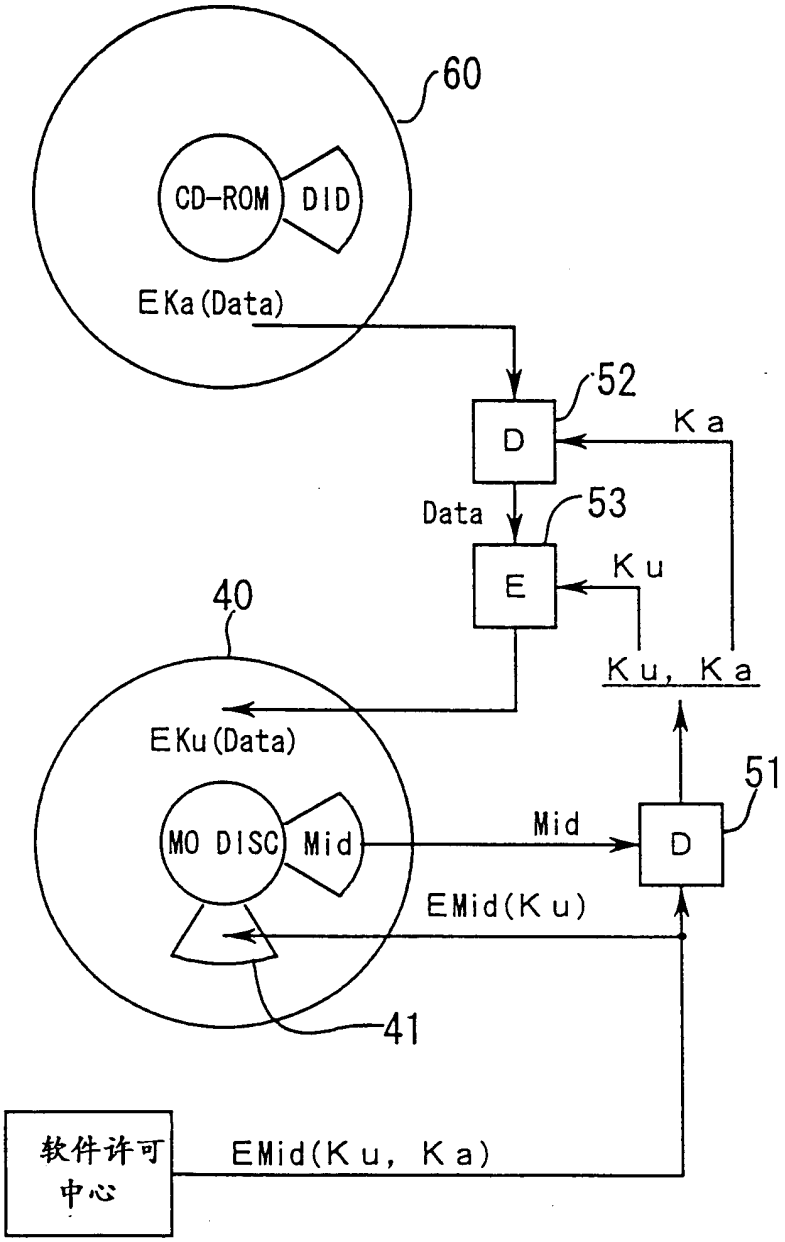

60
CD-ROM
DID
EKa(Data)
52
D
Ka
Data
53
E
Ku
40
Ku, Ka
EKu(Data)
51
MO DISC
Mid
Mid
D
EMid(Ku)
41
软件许可中心
EMid(Ku, Ka)

图 9

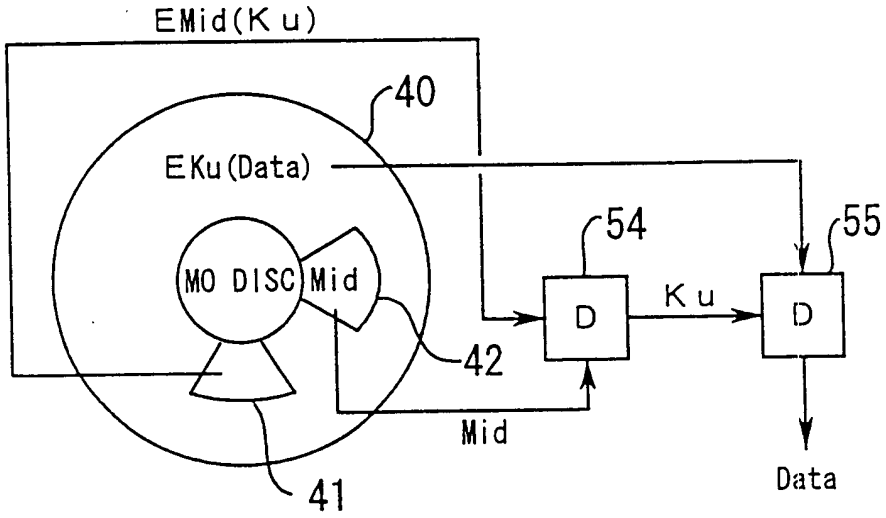


图 10