[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410033368.4

[45] 授权公告日 2007 年 5 月 16 日

[11] 授权公告号 CN 1316379C

[22] 申请日 2004.4.2
[21] 申请号 200410033368.4
[30] 优先权
[32] 2003. 4. 3 [33] JP [31] 099835/2003
[73] 专利权人 索尼株式会社
地址 日本东京
[72] 发明人 粟井昌一
[56] 参考文献
CN1154512A 1997.7.16
审查员 乔凌云

[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 李德山

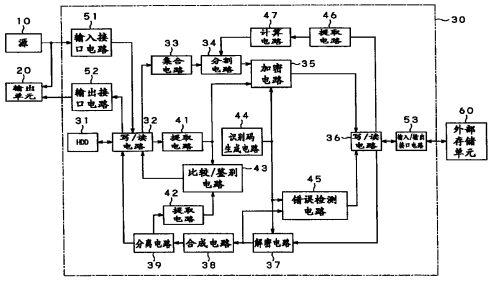
权利要求书 2 页 说明书 9 页 附图 2 页

[54] 发明名称

数据服务装置

[57] 摘要

本发明提供一种数据服务装置，其中包括：将数字数据存储为一个文件的存储单元(31)，将数字数据加密为加密数据的加密电路(35)，将加密数据解密为初始数字数据的解密电路(37)。 对于备份，存储在存储单元(31)中的文件在存储到外部存储单元(60)中之前，被加密电路(35)加密成为加密的文本数据文件。 对于解密，加密数据文件被从外部存储单元中提取出来，由解密电路(37)解密成初始的数字数据，并被写回到存储单元(31)中。 这样，数据服务装置就能既安全又容易地备份存储文件到外部存储单元中。



1. 一种数据服务装置，包括:

用于存储数字数据的存储器件;

用于将数字数据加密成加密数据的加密电路; 以及

用于将加密数据解密成其初始数字数据的解密电路，其中:

从存储在存储器件中的数字数据中提取要被备份的数字数据，通过加密电路加密成加密数据，并存储到外部存储单元中; 且

从存储在外部存储单元的加密数据中提取要被解密的加密数据，通过解密电路解密成初始的数字数据，并写回到存储器件中，

所述的数据服务装置还包括: 比较电路，该比较电路用于对存储器件中的数字数据和存储在外部存储单元中的数据之间的属性数据进行比较，其中:

根据比较电路的比较结果，把存储在存储器件中的数字数据中的、先前已在外部存储单元中备份之后又被更新了的数字数据存储到外部存储单元中。

2. 根据权利要求 1 所述的数据服务装置，还包括: 用于生成对装置本身是唯一的识别码的识别码生成电路，其中:

加密电路根据由识别码生成电路生成的识别码执行加密; 且

解密电路根据由识别码生成电路生成的识别码执行解密。

3. 根据权利要求 2 所述的数据服务装置，还包括: 错误检测电路，该错误检测电路用于在从加密数据中解密数字数据时，根据由识别码生成电路生成的识别码检查数字数据，并在通过检查发现该数字数据被搞错时禁止初始数字数据被写回到存储器件中。

4. 根据权利要求 1-3 中的任一项所述的数据服务装置，还包括:

用于检测作为文件存储到外部存储单元的数字数据的最佳文件的检测电路;

用于将多个文件集合为一个文件的集合电路;

用于将一个文件分割成多个具有预定大小的文件的分割电路;

用于将分割开的文件结合为一个文件的合成电路；以及

用于将由多个文件形成的一个文件分离成多个文件的分离电路，其中：

对于备份数字数据：

由集合电路从存储器件中读取的数字数据被集合为一个文件；

作为集合结果的文件根据检测电路检测出的大小被分割电路进行分割；且

作为分割结果的文件被存储到外部存储单元中；以及

对于解密数字数据：

存储在外部存储单元中的加密数据被加密，然后被合成电路结合为它的初始的一个文件；以及

作为合成结合结果的文件被分离电路分离为多个初始数字数据，并被写回到存储器件中。

5. 根据权利要求 **1-3** 中的任一项所述的数据服务装置，还包括：用于与外部授权服务器进行信息通信的通信电路，其中：

关于解密的数字数据是否要被恢复的询问通过该通信电路传送给外部授权服务器，且只有在通信电路收到来自外部授权电路的恢复允许时才进行恢复操作。

6. 根据权利要求 **4** 所述的数据服务装置，还包括：用于与外部授权服务器进行信息通信的通信电路，其中：

关于解密的数字数据是否要被恢复的询问通过该通信电路传送给外部授权服务器，且只有在通信电路收到来自外部授权电路的恢复允许时才进行恢复操作。

数据服务装置

技术领域

本发明涉及一种数据服务装置，该数据服务装置被设计成用来把各种数字数据备份到外部存储单元中。

本申请要求以 2003 年 4 月 3 日提交的日本专利申请 No.2003－099835 为优先权，其全部内容在此引作参考。

背景技术

随着数字处理和网络技术的发展，已提出了通过广播和网络向用户分发视频和音频数据的技术。而且，还提出了 AV（音频和视频）装置（也被称为“AV 服务器”），该 AV 装置把分发的视频和音频数据一次传送到 HDD（硬盘驱动器）等的设备中存储，并在需要时从 HDD 中取出它们以提供给用户（比较日本未审查专利申请公开 No.2003－30018）。

然而，在上述的 AV 单元中对这样存储的数据进行管理是一个问题。也就是说，已经被用户从他或她自己的介质如 DVD 中复制到这个 AV 单元中的数据，即使由于对该 AV 单元的任何错误操作，如意外的擦除等而把数据破坏了,通过从 DVD 中再次复制，数据就能够容易地被恢复。但是，从原始介质复制所有的数据会花费很长的时间，并会有很多麻烦。

而且，例如，如果从网络上购买的数据遭到了如上所述的破坏，为了得到它，必须为再次分发而支付与买丢失的数据相同的钱。

通过在外部存储单元中存储在AV单元中的数据来进行备份能够防止上述麻烦。即，存储在 AV 单元中的数据即使被破坏也能够从外部存储单元中得到恢复。

然而，在这种情况下，必须对备份存储经常进行管理。即，应经

常在已备份的数据和还没被备份的数据中监视哪些数据备份了。同样，备份系统应设计这样的功能，即，对在外部存储单元中已备份的任意错误的或破坏了的数据不应该是可恢复的。这样的数据在从外部存储单元中恢复到 AV 单元时，将可能导致 AV 单元出故障。

此外，应只有最初的 AV 单元能够从外部存储单元中恢复已备份的数据。如果备份了的数据能够被恢复或复制到与该外部存储单元连接的该最初单元之外的其它 AV 单元，则会出现这样的数据可能被非法复制的问题。

发明内容

因此，本发明的目的在于，通过提供一种能够把各种数字数据备份到外部存储单元中的数据服务装置，来克服上述背景技术中提到的缺点。

上述目的可通过如下实现，即，根据本发明，提供一种数据服务装置，包括：用于存储数字数据的存储器件；用于将数字数据加密成加密数据的加密电路；以及用于将加密数据解密成其初始数字数据的解密电路，其中：从存储在存储器件中的数字数据中提取要被备份的数字数据，通过加密电路加密成加密数据，并存储到外部存储单元中；且从存储在外部存储单元的加密数据中提取要被解密的加密数据，通过解密电路解密成初始的数字数据，并写回到存储器件中，所述的数据服务装置还包括：比较电路，该比较电路用于对存储器件中的数字数据和存储在外部存储单元中的数据之间的属性数据进行比较，其中：根据比较电路的比较结果，把存储在存储器件中的数字数据中的、先前已在外部存储单元中备份之后又被更新了的数字数据存储到外部存储单元中。

在上面的数据服务装置中，把存储在存储器件中的数字数据以加密的状态备份到外部存储单元中。

根据本发明，即使存储在数据服务装置中的原始文件被破坏或损坏，它也能被容易地恢复。例如，即使从网络上购买的一个文件被损坏，它也能被容易地恢复，而不用再次购买该文件。同样，不用对每个文件或目录管理介质，这使得备份原始文件变得容易。

此外，由于原始文件在备份之前被加密，那么，即使该文件被其他任何人非法复制，它的内容也能够得到保护。同样，它能够防止对数据服务装置的系统结构和在数据服务装置中的数据结构的分析。而

且，因为原始文件在提供给外部存储单元之前被加密了，则外部存储单元可以是普通的设备。

而且，如果要在外部存储单元中备份的文件在备份前被搞错了，该文件将不能被恢复到数据服务装置，由此可以确保操作是稳定的。此外，因为对数据服务装置本身是唯一的识别码是被加密和解密的，这就可以防止通过外部存储单元非法复制该文件。而且，因为只有更新的文件被自动地备份，备份操作也缩短了时间。

此外，因为要备份的多个文件被一次集成为一个文件，这就可能避免小容量文件的不连续地备份，这将导致随后的数据处理更有效率。而且，因为要存储到外部存储单元中的一个文件被再分为具有存储到外部存储单元的最佳的文件大小，后者更有效率。

本发明的这些目的和其他目的、特征、优点，从下面的结合附图进行的对优选实施方式的详述中可以清楚地看到。

附图说明

图 1 是本发明的一个实施方式的示意框图；和

图 2 也是本发明的另一个实施方式的示意框图。

具体实施方式

（1） 系统构造和工作

现在看图 1，它示意性地示出了作为本发明的一个实施方式的 AV（音频和视频）服务器的框图。该 AV 服务器通常用附图标记 30 表示。在图 1 中，附图标记 10 表示各种音频和视频信号源中的一个，20 表示图像和声音的输出单元，附图标记 60 表示外部存储单元。

在本实施方式中，源 10 是 DVD 播放器、TV 广播调谐器、CD（压缩盘）播放器等。它向 AV 服务器 30 提供数字数据，如视频和音频信号。输出单元 20 包括显示器和扬声器（没有图示）。从源 10 或 AV 服务器 30 向输出单元 20 提供数字数据，输出单元 20 以图像或声音的形式输出该数字数据。

AV 服务器 30 用来以文件形式存储由源 10 提供的数字数据，这在后面详述。它包括作为大容量的存储器件的 HDD（硬盘驱动器）31，比如有 80GB（十亿字节）的容量。外部存储单元 60 用来备份存储在 AV 服务器 30 中的数字数据。例如，它是可以买到的 USB 连接类型的外部 HDD（“USB”代表“通用串行总线”）。

当 AV 服务器 30 存储从源 10 提供的数字数据时，该数字数据通过输入接口电路 51 被提供给写/读电路 32，并被写入到 HDD31。注意，数字数据的写/读与数据写入到普通的个人电脑中相似。因此，一系列的数字数据作为文件被写入到 HDD31，其中数据以文件形式管理。

而且，当存储在 AV 服务器 30 中的（数字数据的）文件要被使用时，由写/读电路 32 从 HDD31 中读出对象或想要的文件，这样读出的文件中的数字数据通过输出接口电路 52 被提供给输出单元 20，或者作为图像或声音再现。

（2） AV 服务器 30 的构造和工作（Ⅰ）

如上所述，AV 服务器 30 把从源 10 提供的数字数据存储到 HDD31 中，并把它从 HDD31 提供给输出单元 20。为了将存储在 HDD31 中的数字数据备份到外部存储单元 60 中，并从外部存储单元 60 恢复已备份的数字数据，AV 服务器 30 的结构和功能如下所述。

（2－1）备份和恢复概述

为了在 HDD31 中备份（数字数据的）文件，写/读电路 32 从 HDD31 中顺序读文件。这样读出的文件被提供给集合电路 33。提供给集合电路 33 的多个文件将被集合为一系列的文件。

当来自集合电路 33 的系列文件被提供给分割电路 34 以便存储到外部存储单元 60 中去时，文件被分割电路 34 分割为多个文件，每一个文件具有适宜存储的最佳大小。作为分割结果的文件被提供给加密电路 35，在这里文件被加密成为加密的文本文件。该加密的文本文件通过写/读电路 36 和输入/输出接口电路 53 提供给外部存储单元 60，并被存储在这里。需要注意的是，在外部存储单元 60 中，数据被存储的形式与在用于个人电脑等中的 HDD 中的数据存储形式类似。即，

一个加密文本文件被作为一个文件存储。

这样，HDD31 中的文件就被备份在外部存储单元 60 中。

与之相反，为了把在外部存储单元 60 中备份的文件恢复到 HDD31 中，加密文本文件被从外部存储单元 60 中顺序读出，并先通过输入/输出接口电路 53，然后通过写/读电路 36 提供给解密电路 37，并在这里被解密为初始的数字数据文件。

然后，文件被提供给合成电路 38，该合成电路 38 把文件结合成一个与由集合电路 33 提供的文件相似的文件。这样合成的文件被提供给分离电路 39，该分离电路 39 把该文件分离成初始的文件，这些文件通过写/读电路 32 被写回到 HDD31。

这样，在外部存储单元 60 中备份的文件就被恢复到 HDD31。

（2－2）备份和恢复的详细描述

为了正确地进行数据备份和恢复，AV 服务器 30 将如下所述地构成。即，提取电路 41 被连接到写/读电路 32。对于备份操作，从提取电路 41 提取表示 HDD31 中的每一个文件属性的数据，如表示文件名、文件大小、存储日期等的数据，并把它提供给比较电路 43。而正如后面要详述的那样，在外部存储单元 60 那里也存储了备份的文件（已存储在 HDD31 中的文件）的属性数据。还有另一个提取电路 42 连接到分离电路 39。它提取在外部存储单元 60 中备份的文件的属性数据（初始文件已经被存储在 HDD31 中，并被提供给外部存储单元 60 作备份）。这样提取的属性数据被提供给比较电路 43。

在比较电路 43 中，从提取电路 41 和 42 提供的文件属性数据在此一一进行比较，以鉴别出在外部存储单元 60 中备份的每一组文件，以及哪些在先前备份后又被更新（HDD31 中的文件）。鉴别的结果被提供给写/读电路 32，在写/读电路 32 中，只有那些在先前备份后又被更新的文件会从 HDD31 中读出，并如前文所述地被备份到外部存储单元 60 中。此时，存储在外部存储单元 60 中的属性数据也被相应地更新为在外部存储单元 60 中备份的内容。

因此，存储在 HDD31 中的文件被备份到外部存储单元 60 中，但

是，存储在 HDD31 中，且先前已经备份之后没有再更新的文件不会被再次备份到外部存储单元 60 中。即，只有那些在 HDD31 中更新了的文件（包括重新存储的文件）将被重新备份。

此外，AV 服务器 30 包括连接到另一个写/读电路 36 的提取电路 46。提取电路 46 提取表示外部存储单元 60 的写/读特性的数据，比如用于表示簇大小和轨道大小的数据，并提供给文件大小计算电路 47，该文件大小计算电路 47 计算用于读出或写入外部存储单元 60 的最佳大小值，并将表示该最佳大小的数据提供给分割电路 34。

由此，在备份操作中，如上所述，根据由文件大小计算电路 47 计算出的最佳大小值，分割电路 34 将来自集合电路 35 的文件分割为多个文件，其中每一个文件都具有用来存储到外部存储单元 60 中的最佳大小值。

AV 服务器 30 还包括识别码生成电路 44，它提取对 AV 服务器 30 本身是唯一的识别码，例如，MAC（介质存取控制）地址，或者是用户给每一个 AV 服务器 30 分配的唯一的识别码，该识别码生成电路 44 把识别码提供给加密电路 35 作为加密密钥数据。这样，在备份操作期间，加密电路 35 按照识别码生成电路 44 提供的识别码，将分割电路 34 提供的文件加密成为加密的数据文件。

对于恢复操作，识别码生成电路 44 向解密电路 37 提供识别码，该解密电路 37 根据所提供的识别码，把从外部存储单元 60 提取出并提供给解密电路 37 的加密数据文件解密成初始数字数据的文件。

然而，在上述解密期间，被解密的文件和来自识别码生成电路 44 的识别码被提供给错误（falsification）检测电路 45，该错误检测电路 45 检查从外部存储单元 60 中提取的文件是否有错误。如果这个文件被发现有错误，该错误检测电路 45 提供一个错误检测输出，它将控制写/读电路 36 停止从外部存储单元 60 得到加密数据。换句话说，向 HDD31 写入解密文件的操作将被禁止。

与之相反，当从外部存储单元 60 中提取的文件被发现没有错误，由如上所述的解密电路 37 解密的文件将被提供给分离电路 39，该分

离电路 39 把文件分离为初始文件，然后写回到 HDD31 中。

由此，如图 1 所示的 AV 服务器 30 将 HDD31 中的文件备份到外部存储单元 60 中。这样，即使在 HDD31 中的任一文件被破坏或损坏了，它也能被容易地恢复。举例来说，即使一个从网络上购买的文件，它也能够被容易地恢复，而不用再次购买该文件。而且，因为 HDD31 中的所有的文件被备份在一个外部存储单元 60 中，所以不用对每一个文件或内容管理备份介质，它也有利于容易地备份。

此外，因为 HDD31 中的文件在备份到外部存储单元 60 之前要被加密，即使其他任何人复制外部存储单元 60 中的任一文件到个人电脑等中，它的内容也能够得到保护。而且，它也能防止对 AV 服务器 30 的系统结构和在 AV 服务器 30 中的数据结构的分析。而且，因为 HDD31 中的文件在提供给外部存储单元 60 备份之前被加密，该外部存储单元 60 可以是普通的设备。

而且，如果备份到外部存储单元 60 的文件被搞错了，它将不被恢复到 AV 服务器 30。这样，可以确保对 AV 服务器 30 的操作是稳定的。

而且，即使通过将第一个 AV 服务器 30 连接到第二个 AV 服务器 30，试图从第一个 AV 服务器 30 中备份一个文件到第二个 AV 服务器 30，然后把第一个 AV 服务器 30 中的文件恢复到第二个 AV 服务器 30，从外部存储单元 60 中到第二个 AV 服务器 30 的文件恢复也将是不被接受的，这是因为该文件是根据对每一台 AV 服务器 30 的唯一的识别码来加密和解密的。因此，即使使用另一台与该 AV 服务器有同样构造的 AV 服务器，也能够防止从外部存储单元 60 中非法复制任一文件给这样的 AV 服务器。

而且，因为比较/鉴别电路 43 比较 HDD31 中的文件和外部存储单元 60 中的文件的属性数据，这样，只有更新了的文件会被备份，文件的备份工作时间就缩短了。

此外，因为在 HDD31 中的要被备份的多个文件被一次集合为一个文件，它也可能避免容量小的文件不连续地备份，这就使随后的备

份所做的数据处理更有效率。同样，因为存储在外部存储单元 60 中的一个文件被再分为具有最佳的文件大小而存储到外部存储单元 60，这样，存储将更有效率。

（3）AV 服务器 30 的构造和工作（Ⅱ）

现在看图 2，它示意性地示出了作为本发明的数据服务装置的另一个实施方式的框图。如图 2 所示，这个 AV 服务器通常也用附图标记 30 表示，它也使用外部存储单元 60 和授权服务器 70。在图 2 中也能看到，这个 AV 服务器除了有如图 1 中的 AV 服务器 30 的组件外，还包括通信电路 54。当把外部存储单元 60 中备份的数据恢复到 HDD31 中时，通过通信电路 54，将来自于要恢复的数据和该 AV 服务器 30 的识别码相结合产生的信息传送给授权服务器 70。要注意的是，通信电路 54 能够通过诸如互联网(Internet)等网络连接到授权服务器 70，并以加密方式与授权服务器 70 进行通信。

结果，只有当收到来自授权服务器 70 的恢复允许时，在外部存储单元 60 中备份的文件才能被恢复到 HDD31。同样，如果授权服务器 70 发出恢复不允许，AV 服务器 30 将在显示器上警告。因此，这个 AV 服务器 30 能够防止备份在外部存储单元 60 中的文件被非法复制。

而且，因为在通信电路 54 和授权服务器 70 之间的通信是加密的，并且甚至是非法地截取或解密数据也具有取决于要恢复的数据的一个值，它不可能独自地提取该 AV 服务器 30 的识别码，这样在该 AV 服务器里的任意的用户信息就不会被泄漏了。

（4）其它

前面，结合附图，以具体的优选实施方式作为例子详细描述了本发明的情况。然而，本领域的一般技术人员可以理解，本发明并不限于这些实施方式，只要不偏离如所附权利要求书中阐述和限定的范围和精神，本发明就能以不同的方式更改和实施。

例如，尽管如前所述，根据本发明，在 AV 服务器中源 10 用来提供视频和音频信号，它也可以是如个人电脑、网络等的能够提供诸

如电子邮件、文本数据、静止或活动图像数据等数字数据的信号源。

同样，AV 服务器可以设计成，当存储在 HDD31 中并将要被备份到外部存储单元 60 的所有文件的大小总和大于外部存储单元 60 所剩容量时，通过显示器警告。

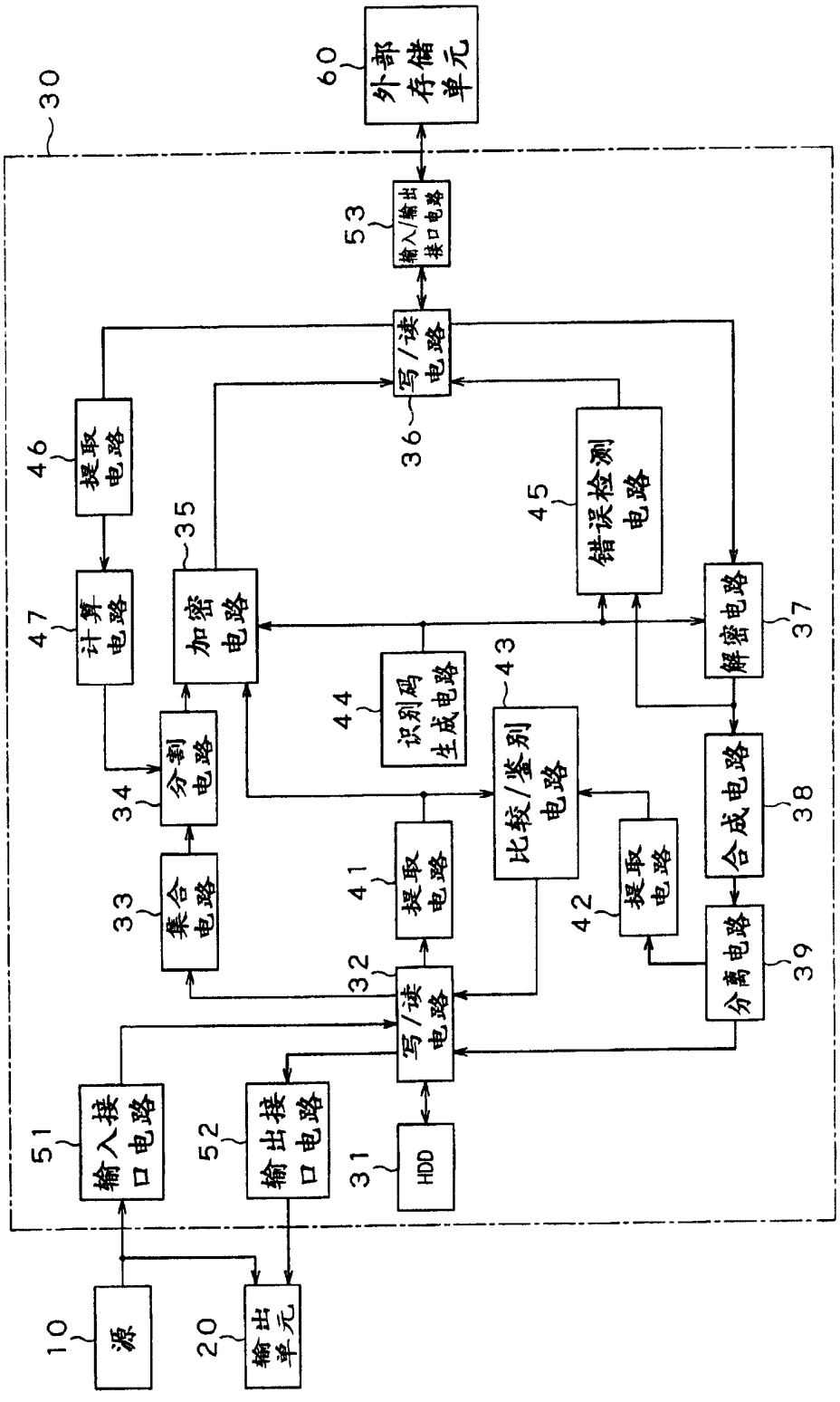

30
60
外部存储单元
53
输入/输出接口电路
写/读电路
36
46
提取电路
47
计算电路
35
加密电路
45
错误检测电路
解密电路
37
44
识别码生成电路
43
34
分割电路
比较/鉴别电路
33
集合电路
41
提取电路
42
提取电路
合成电路
38
32
写/读电路
分离电路
39
51
输入接口电路
52
输出接口电路
31
HDD
10
源
20
输出单元

图1

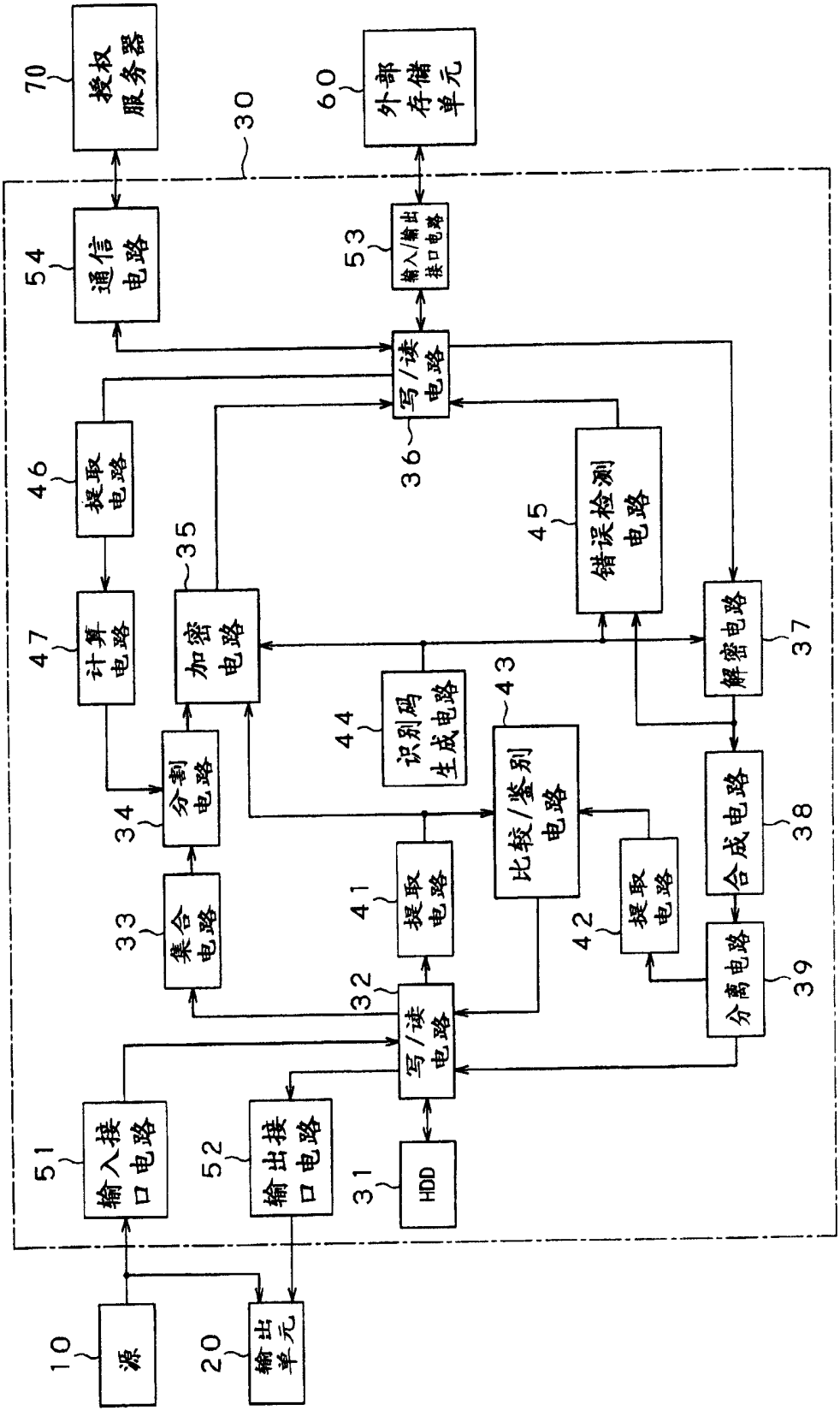

70
授权服务器
30
60
外部存储单元
54
通信电路
53
输入/输出接口电路
写/读电路
36
46
提取电路
45
错误检测电路
35
47
计算电路
加密电路
解密电路
37
44
识别码生成电路
43
34
分割电路
比较/鉴别电路
33
集合电路
41
提取电路
42
提取电路
合成电路
38
32
写/读电路
分离电路
39
51
输入接口电路
52
输出接口电路
31
HDD
10
源
20
输出单元

图2