(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 101957901 B
(45)授权公告日 2014.06.04

(21)申请号 200910160009.8
(22)申请日 2009.07.15
(73)专利权人 精品科技股份有限公司
地址 中国台湾新竹市
(72)发明人 郭耿言
(74)专利代理机构 上海波拓知识产权代理有限公司 31264
代理人 杨波
(51)Int.Cl.
G06F 21/78(2013.01)
G06F 21/62(2013.01)

(56)对比文件
WO 2009012613 A1,2009.01.29,
CN 101443756 A,2009.05.27,
CN 101452454 A,2009.06.10,
US 2009178123 A1,2009.07.09,

审查员 吴广平

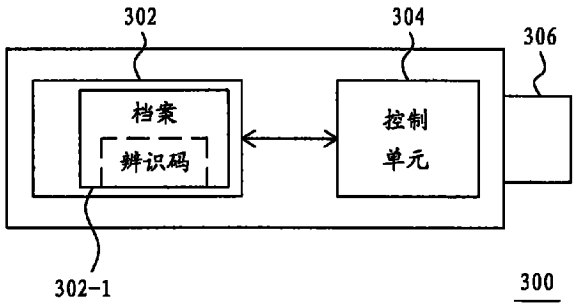
权利要求书1页 说明书6页 附图3页

(54)发明名称

外接式储存装置及其制造方法、其资讯安全管理方法

(57)摘要

本发明是有关一种外接式储存装置及其制造方法、外接式储存装置的资讯安全管理方法。所述外接式储存装置的存储单元储存有一档案，此档案具有一识别码。此识别码可被安装有一资讯安全管理软件的电脑辨识，而此资讯安全管理软件会使电脑依据识别码而赋予外接式储存装置对应的数据存取权限。在所述制造方法中，是在一外接式储存装置的存储单元中储存上述的档案。此外，在所述的资讯安全管理方法中，是利用上述的资讯安全管理软件，来判断连接至电脑的一外接式储存装置是否具有上述档案，以决定是否使电脑赋予此外接式储存装置对应的数据存取权限。



CN 101957901 B

1. 一种外接式储存装置，其特征在于其包括：

一连接介面；以及

一存储单元，储存有一档案，该档案具有一识别码，该识别码仅可被安装有一资讯安全管理软件的一电脑辨识，而该资讯安全管理软件会使该电脑依据该识别码而赋予该外接式储存装置对应的数据存取权限，从而管控该电脑与该外接式储存装置之间的数据存取行为，其中该外接式储存装置与该电脑是互相独立的两个电子装置。

2. 根据权利要求 1 所述的外接式储存装置，其特征在于其中所述的档案是一文本文档。

3. 根据权利要求 1 所述的外接式储存装置，其特征在于其中所述的连接介面是一 USB 连接介面。

4. 一种外接式储存装置的制造方法，其特征在于其包括以下步骤：

提供一外接式储存装置，其中该外接式储存装置具有一存储单元；以及

在该存储单元中储存一档案，该档案具有一识别码，该识别码仅可被安装有一资讯安全管理软件的一电脑辨识，而该资讯安全管理软件会使该电脑依据该识别码而赋予该外接式储存装置对应的数据存取权限，从而管控该电脑与该外接式储存装置之间的数据存取行为，其中该外接式储存装置与该电脑是互相独立的两个电子装置。

5. 根据权利要求 4 所述的外接式储存装置的制造方法，其特征在于其中所述的档案是一文本文档。

6. 根据权利要求 4 所述的外接式储存装置的制造方法，其特征在于其中所述的连接介面是一 USB 连接介面。

7. 一种外接式储存装置的资讯安全管理方法，适用于一电脑，该电脑安装有一资讯安全管理软件，其特征在于该方法包括以下步骤：

利用该资讯安全管理软件判断该电脑所连接的一外接式储存装置的一存储单元中，是否储存了具有一识别码的一档案，该识别码仅可被安装有该资讯安全管理软件的该电脑辨识；以及

当判断为是时，利用该资讯安全管理软件取得该识别码，并确认该识别码是否属于该资讯安全管理软件所预设的多个管控识别码的其中之一，以决定是否使该电脑依据该识别码而赋予该外接式储存装置对应的数据存取权限，从而管控该电脑与该外接式储存装置之间的数据存取行为，其中该外接式储存装置与该电脑是互相独立的两个电子装置。

8. 根据权利要求 7 所述的外接式储存装置的资讯安全管理方法，其特征在于其中当该识别码属于该资讯安全管理软件所预设的多个管控识别码的其中之一时，该资讯安全管理软件便使该电脑依据该识别码而赋予该外接式储存装置对应的数据存取权限。

9. 根据权利要求 7 所述的外接式储存装置的资讯安全管理方法，其特征在于其中当该识别码不属于该资讯安全管理软件所预设的多个管控识别码的其中之一时，该资讯安全管理软件便限制该电脑与该外接式储存装置之间的数据存取行为。

10. 根据权利要求 7 所述的外接式储存装置的资讯安全管理方法，其特征在于其中当该存储单元中，并没有储存具有该识别码的该档案时，该资讯安全管理软件便限制该电脑与该外接式储存装置之间的数据存取行为。

外接式储存装置及其制造方法、其资讯安全管理方法

技术领域

[0001] 本发明是有关于资讯安全领域的技术，且特别是有关于一种外接式储存装置及其制造方法，以及一种外接式储存装置的资讯安全管理方法。

背景技术

[0002] 近年来，许多公司纷纷采用资讯安全 (information security) 管理系统，以保护公司内部的重要数据，避免重要数据外流而造成公司的重大损失。图 1 是资讯安全管理系统的其中一种架构示意图。请参照图 1，此架构包括有资讯安全服务器 102、AD(active directory，译为目录服务）服务器 104、数据库 (database)106 及控制台 (console)108。其中，资讯安全服务器 102 安装有资讯安全管理软件。上述这些设备是通过公司内部网路 110 而与电脑 112、114、116、118 及 120 连接，且这些电脑都安装有前述资讯安全管理软件的代理程序 (agent)。管理者可通过控制台 108 来对数据库 106 设定上述电脑的数据存取权限，以便让资讯安全管理系统管理这些电脑的数据（或称资料）存取行为（详后述）。

[0003] 图 2 是现有习知的一种应用于前述资讯安全管理系统的 USB 随身盘架构示意图。所谓 USB 随身盘即是 USB flash drive，其中 USB 为 universalserial bus 的缩写，译为通用串列汇流排。请参照图 2，此 USB 随身盘 200 包括有存储单元 202、控制单元 204 及 USB 连接介面 206。存储单元 202 具有一存储空间，此存储空间即是一般用以供使用者置放档案的空间。而此存储空间被划分为隐藏空间 202-1 及开放空间 202-2 这两个部分，且隐藏空间 202-1 内设有识别码 (identification code，ID code)。当 USB 随身盘 200 通过其 USB 连接介面 206 而连接至电脑时，电脑只会显示出开放空间 202-2 内的储存内容，而不会显示出隐藏空间 202-1 内的储存内容。

[0004] 前述的资讯安全管理系统分有两种操作方式，其中第一种操作方式是必须以随时连线的方式来进行操作，而第二种操作方式则是不必随时连线也可进行操作。请参照图 1 及图 2 来说明第一种操作方式。当有员工将 USB 随身盘 200 连接至图 1 中的任一电脑，例如连接至电脑 116 时，电脑 116 中的资讯安全管理软件的代理程序，就会去取得 USB 随身盘 200 的隐藏空间 202-1 内的识别码，并将有一 USB 随身盘连接至电脑 116 的情况，以及 USB 随身盘 200 的识别码告知资讯安全服务器 102。接着，资讯安全服务器 102 便会向 AD 服务器 104 确认电脑 116 是否属于公司内部管控的电脑。

[0005] 承上述，一但确认为是，资讯安全服务器 102 就会转而向数据库 106 确认 USB 随身盘 200 的识别码，以判断此识别码是否属于管理者事先通过控制台 108 输入至数据库 106 的内部管控识别码。若又确认为是，那么资讯安全服务器 102 就会向数据库 106 取得对应于 USB 随身盘 200 的识别码的数据存取权限，并将此数据存取权限告知电脑 116。如此一来，电脑 116 中的资讯安全管理软件的代理程序，便可根据 USB 随身盘 200 的识别码的数据存取权限，来管控电脑 116 与 USB 随身盘 200 之间的数据存取行为。

[0006] 接着将继续说明第二种方式，请再参照图 1 及图 2。当有员工将 USB 随身盘 200 连接至图 1 中的任一电脑，例如连接至电脑 116 时，电脑 116 中的资讯安全管理软件的代理

程序，就会去取得USB随身盘200的隐藏空间202-1内的识别码，并将取得的辨识码与电脑116事先储存的公司内部所有的管控识别码来做比对。这些管控识别码可由管理者事先通过控制台108来对数据库106进行设定，并于设定这些管控识别码的同时给定每一管控识别码对应的数据存取权限，进而让资讯安全服务器102可于设定完毕后将这些管控识别码及每一管控识别码对应的数据存取权限部署至电脑112、114、116、118及120。

[0007] 因此，在代理程序取得识别码之后，一但代理程序判断所取得的识别码是属于公司内部管控识别码的其中之一时，代理程序就会依照此识别码对应的数据存取权限来管控电脑116与USB随身盘200之间的数据存取行为。反之，若代理程序判断所取得的识别码并不属于公司内部管控识别码时，代理程序就会限制电脑116与USB随身盘200之间的数据存取行为。而此处所指的限制，例如是禁止电脑116将档案储存至USB随身盘200，但电脑116仍可读取储存在USB随身盘200中的档案。

[0008] 尽管使用图2所示型式的USB随身盘，有利于公司内部的资讯安全管控，然而由上述的说明可知，前述形式的USB随身盘乃是特制的USB随身盘，故必须有USB随身盘制造商愿意配合设计及生产才行。此外，在图2所示的USB随身盘200中，所采用的控制单元204也必须具有可将存储单元202的存储空间，划分为隐藏空间202-1及开放空间202-2这两个部分的功能，故也必须有控制单元制造商愿意配合设计及生产才行。这么一来，就会导致采用资讯安全管理系统的这些公司，必须再额外花费一笔钱去订做特制的USB随身盘，且也不见得花钱就买得到。

发明内容

[0009] 本发明的目的就是在提供一种外接式储存装置，其适合与资讯安全管理系统搭配使用，并且容易制造。

[0010] 本发明的另一目的就是在提供一种外接式储存装置的制造方法，其可制造出适合与资讯安全管理系统搭配使用的外接式储存装置，且制造过程快速，制造成本也低廉。

[0011] 本发明的再一目的就是在提供一种外接式储存装置的资讯安全管理方法，其可使电脑能判断与其连接的外接式储存装置是否属于公司内部管控的外接式储存装置，据以决定是否赋予此外接式储存装置对应的数据存取权限。

[0012] 本发明的目的及解决其技术问题是采用以下技术方案来实现的。依据本发明提出的一种外接式储存装置，其包括有连接介面及存储单元。此存储单元储存有一档案，而此档案具有一识别码。所述识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使电脑依据识别码而赋予外接式储存装置对应的数据存取权限。

[0013] 本发明的目的及解决其技术问题还采用以下技术方案来实现。依据本发明提出的一种外接式储存装置的制造方法。在此方法中，首先是提供一外接式储存装置，此外接式储存装置具有存储单元。接着，在上述存储单元中储存一档案，而此档案具有一识别码。所述识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使电脑依据识别码而赋予外接式储存装置对应的数据存取权限。

[0014] 本发明的目的及解决其技术问题另外再采用以下技术方案来实现。依据本发明提出的一种外接式储存装置的资讯安全管理方法，适用于一电脑，而此电脑安装有资讯安全管理软件。在此方法中，首先是利用资讯安全管理软件判断此电脑所连接的一外接式储

存装置的存储单元中，是否储存了具有一识别码的一档案。接着，当判断为是时，利用资讯安全管理软件取得识别码，并确认识别码是否属于资讯安全管理软件所预设的多个管控识别码的其中之一，以决定是否使电脑依据识别码而赋予外接式储存装置对应的数据存取权限。

[0015] 本发明的目的及解决其技术问题还可采用以下技术措施进一步实现。

[0016] 在本发明的一实施例中，上述的档案包括是一文本文档。

[0017] 在本发明的一实施例所述的资讯安全管理方法中，当识别码属于资讯安全管理软件所预设的多个管控识别码的其中之一时，资讯安全管理软件便使电脑依据识别码而赋予上述外接式储存装置对应的数据存取权限。

[0018] 在本发明的一实施例所述的资讯安全管理方法中，当识别码不属于资讯安全管理软件所预设的多个管控识别码的其中之一时，资讯安全管理软件便会限制电脑与上述外接式储存装置之间的数据存取行为。

[0019] 在本发明的一实施例所述的资讯安全管理方法中，当上述外接式储存装置的存储单元中，并没有储存具有识别码的档案时，资讯安全管理软件便会限制电脑与上述外接式储存装置之间的数据存取行为。

[0020] 本发明与现有技术相比具有明显的优点和有益效果。借由上述技术方案，本发明外接式储存装置及其制造方法、外接式储存装置的资讯安全管理方法至少具有下列优点及有益效果：本发明乃是在一外接式储存装置的存储单元中储存一档案，此档案具有一识别码，且此识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使电脑依据识别码而赋予外接式储存装置对应的数据存取权限。因此，本发明所提出的外接式储存装置适合与资讯安全管理系统搭配使用，并且容易制造。此外，由于本发明所提出的外接式储存装置容易制造，故制造过程快速，且制造成本也低廉。进一步地，本发明还针对外接式储存装置提出一套资讯安全管理方法，通过辨识与电脑连接的外接式储存装置中是否储存具有识别码的档案，若为是，便又再进一步判别识别码是否属于公司内部的管控识别码，以这样的操作来判别此外接式储存装置是否属于公司内部列管的储存装置，据以决定是要依据识别码而赋予外接式储存装置对应的数据存取权限，还是要限制电脑与外接式储存装置之间的数据存取行为。

[0021] 上述说明仅是本发明技术方案的概述，为了能够更清楚了解本发明的技术手段，而可依照说明书的内容予以实施，并且为了让本发明的上述和其他目的、特征和优点能够更明显易懂，以下特举较佳实施例，并配合附图，详细说明如下。

附图说明

[0022] 图 1 是现有资讯安全管理系统的其中一种架构示意图。

[0023] 图 2 是现有习知的一种应用于前述资讯安全管理系统的 USB 随身盘架构示意图。

[0024] 图 3 是本发明外接式储存装置较佳实施例的示意图。

[0025] 图 4 是本发明外接式储存装置的制造方法较佳实施例的流程示意图。

[0026] 图 5 是本发明外接式储存装置的资讯安全管理方法较佳实施例的流程示意图。

[0027] 102：资讯安全服务器 104：AD 服务器

[0028] 106：数据库 108：控制台

[0029] 110 :内部网路 112、114、116、118、120 :电脑

[0030] 200、300 :外接式储存装置 202、302 :存储单元

[0031] 202-1 :隐藏空间 202-2 :开放空间

[0032] 204、304 :控制单元 206 :USB 连接介面

[0033] 302-1 :档案 306 :连接介面

[0034] S402、S404、S502、S504、S506、S508、S510 :步骤

具体实施方式

[0035] 为更进一步阐述本发明为达成预定发明目的所采取的技术手段及功效，以下结合附图及较佳实施例，对依据本发明提出的外接式储存装置及其制造方法、外接式储存装置的资讯安全管理方法其具体实施方式、结构、方法、步骤、特征及其功效，详细说明如后。

[0036] 请参照图 3 所示，是本发明外接式储存装置较佳实施例的示意图。本发明较佳实施例的外接式储存装置 300 包括 :存储单元 302、控制单元 304 及连接介面 306。其中，存储单元 302 储存有档案 302-1，此档案 302-1 例如是一个文本文档。而档案 302-1 具有识别码，此识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使前述电脑依据识别码而赋予外接式储存装置 300 对应的数据存取权限。简明来说，此外接式储存装置 300 的存储单元 302 的存储空间并未被划分成隐藏空间及开放空间这两个部分，而是直接储存具有识别码的档案 302-1。

[0037] 因此，资讯安全管理软件可使电脑依据上述识别码对应的数据存取权限，来管控电脑本身与外接式储存装置 300 之间的数据存取行为，例如限制电脑不能将电脑中的数据储存至外接式储存装置 300，又或者是限制电脑不能将外接式储存装置 300 中的数据储存至电脑中。

[0038] 假若外接式储存装置 300 是一个 USB 随身盘，则其连接介面 306 就是一个 USB 连接介面。而相较于在现有技术所提及的 USB 随身盘 200，此外接式储存装置 300 的存储单元 302 的存储空间并不需要被划分为隐藏空间及开放空间这两个部分，且此外接式储存装置 300 所采用的控制单元 304，也不必具有可将存储单元 302 的存储空间划分为隐藏空间及开放空间的功能。如此，便显得外接式储存装置 300 很容易制造。此外，若此外接式储存装置 300 是 USB 随身盘以外的储存装置，那么外接式储存装置 300 也可能不具有控制单元 304。

[0039] 请参照图 4 所示，是本发明外接式储存装置的制造方法较佳实施例的流程示意图。本发明较佳实施例的外接式储存装置的制造方法，首先是提供一外接式储存装置，其中此外接式储存装置具有存储单元（如步骤 S402 所示）。接着，在上述存储单元中储存一档案，此档案具有一识别码，此识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使前述电脑依据识别码而赋予外接式储存装置对应的数据存取权限（如步骤 S404 所示）。由上述可知，此方法仅需将具有识别码的档案储存在外接式储存装置的存储单元中，故外接式储存装置的制造过程快速，且制造成本也低廉。

[0040] 进一步地，本发明还针对外接式储存装置提出一套资讯安全管理方法。请参阅图 5 所示，是本发明外接式储存装置的资讯安全管理方法较佳实施例的流程示意图。本发明较佳实施例的外接式储存装置的资讯安全管理方法，适用于一电脑，且此电脑安装有资讯安全管理软件。在此方法中，首先是利用资讯安全管理软件判断电脑所连接的外接式储存装

置的存储单元中，是否储存了具有识别码的档案（如步骤 S502 所示）。当外接式储存装置的存储单元中，并没有储存具有识别码的档案时，资讯安全管理软件便会限制电脑与外接式储存装置之间的数据存取行为（如步骤 S506 所示）。而此处所指的限制，例如是禁止电脑将档案储存至外接式储存装置，但电脑仍可读取储存在外接式储存装置中的档案。

[0041] 相反地，当外接式储存装置的存储单元中储存了具有识别码的档案时，便利用资讯安全管理软件取得识别码，并确认识别码是否属于资讯安全管理软件所预设的多个管控识别码的其中之一，以决定是否使电脑依据识别码而赋予外接式储存装置对应的数据存取权限（如步骤 S504 所示）。

[0042] 在执行完步骤 S504 之后，当识别码属于资讯安全管理软件所预设的多个管控识别码的其中之一时，资讯安全管理软件便使电脑依据识别码而赋予外接式储存装置对应的数据存取权限（如步骤 S508 所示）。反之，当识别码不属于资讯安全管理软件所预设的多个管控识别码的其中之一时，资讯安全管理软件便会限制电脑与外接式储存装置之间的数据存取行为（如步骤 S510 所示）。

[0043] 基于上述资讯安全管理方法的教示，图 1 所示的资讯安全管理系统的设计者，便可稍微修改资讯安全服务器 102 所安装的资讯安全管理软件的操作，以及电脑 112、114、116、118 及 120 所安装的资讯安全管理软件的代理程序的操作，让图 3 所示的外接式储存装置 300 适合与图 1 所示的资讯安全管理系统搭配使用。再用以下所述的外接式储存装置 300 与资讯安全管理系统之间的操作方式来举例之。

[0044] 必须先说明的是，在此资讯安全管理方法中，所运用到的资讯安全管理系统亦分有两种操作方式，其中第一种操作方式是必须以随时连线的方式来进行操作，而第二种操作方式则是不必随时连线也可进行操作。请参照图 1 及图 3 来说明第一种操作方式。当有员工将外接式储存装置 300 连接至图 1 中的任一电脑，例如连接至电脑 116 时，电脑 116 中的资讯安全管理软件的代理程序，就会去取得外接式储存装置 300 的存储单元 302 中，所储存的档案 302-1 的识别码，并将有一外接式储存装置连接至电脑 116 的情况，以及外接式储存装置 300 的识别码告知资讯安全服务器 102。接着，资讯安全服务器 102 便会向 AD 服务器 104 确认电脑 116 是否属于公司内部管控的电脑。

[0045] 承上述，一但确认为是，资讯安全服务器 102 就会转而向数据库 106 确认外接式储存装置 300 的识别码，以判断此识别码是否属于管理者事先通过控制台 108 输入至数据库 106 的内部管控识别码。若又确认为是，那么资讯安全服务器 102 就会向数据库 106 取得对应于外接式储存装置 300 的识别码的数据存取权限，并将此数据存取权限告知电脑 116。如此一来，电脑 116 中的资讯安全管理软件的代理程序，便可根据外接式储存装置 300 的识别码的数据存取权限，来管控电脑 116 与外接式储存装置 300 之间的数据存取行为。

[0046] 接着将继续说明第二种方式，请再参照图 1 及图 3。当有员工将外接式储存装置 300 连接至图 1 中的任一电脑，例如连接至电脑 116 时，电脑 116 中的资讯安全管理软件的代理程序，就会去取得外接式储存装置 300 的存储单元 302 中，所储存的档案 302-1 的识别码，并将取得的辨识码与电脑 116 事先储存的公司内部所有的管控识别码来做比对。这些管控识别码可由管理者事先通过控制台 108 来对数据库 106 进行设定，并于设定这些管控识别码的同时给定每一管控识别码对应的数据存取权限，进而让资讯安全服务器 102 可于设定完毕后将这些管控识别码及每一管控识别码对应的数据存取权限部署至电脑 112、

114、116、118 及 120。

[0047] 因此，在代理程序取得识别码之后，一但代理程序判断所取得的识别码是属于公司内部管控识别码的其中之一时，代理程序就会依照此识别码对应的数据存取权限来管控电脑 116 与外接式储存装置 300 之间的数据存取行为。反之，若代理程序判断所取得的识别码并不属于公司内部管控识别码时，代理程序就会限制电脑 116 与外接式储存装置 300 之间的数据存取行为。此处所指的限制，例如是禁止电脑 116 将档案储存至外接式储存装置 300，但电脑 116 仍可读取储存在外接式储存装置 300 中的档案。

[0048] 综上所述，本发明乃是在一外接式储存装置的存储单元中储存一档案，此档案具有一识别码，且此识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使电脑依据识别码而赋予外接式储存装置对应的数据存取权限。因此，本发明所提出的外接式储存装置适合与资讯安全管理系统搭配使用，并且容易制造。此外，由于本发明所提出的外接式储存装置容易制造，故制造过程快速，且制造成本也低廉。进一步地，本发明还针对外接式储存装置提出一套资讯安全管理方法，通过辨识与电脑连接的外接式储存装置中是否储存具有识别码的档案，若为是，便又再进一步判别识别码是否属于公司内部的管控识别码，以这样的操作来判别此外接式储存装置是否属于公司内部列管的储存装置，据以决定是要依据识别码而赋予外接式储存装置对应的数据存取权限，还是要限制电脑与外接式储存装置之间的数据存取行为。

[0049] 以上所述，仅是本发明的较佳实施例而已，并非对本发明作任何形式上的限制，虽然本发明已以较佳实施例揭露如上，然而并非用以限定本发明，任何熟悉本专业的技术人员，在不脱离本发明技术方案范围内，当可利用上述揭示的方法及技术内容作出些许的更动或修饰为等同变化的等效实施例，但凡是未脱离本发明技术方案的内容，依据本发明的技术实质对以上实施例所作的任何简单修改、等同变化与修饰，均仍属于本发明技术方案的范围内。

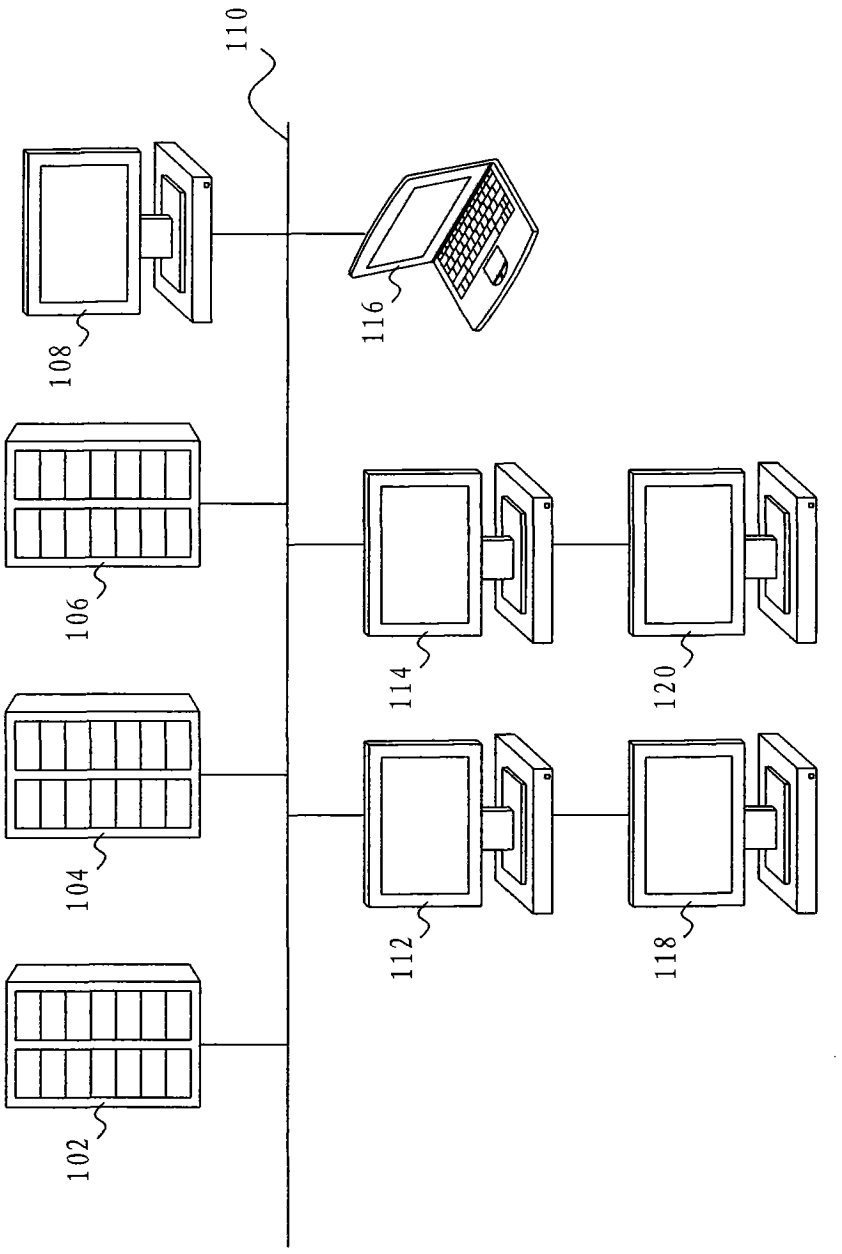


图 1

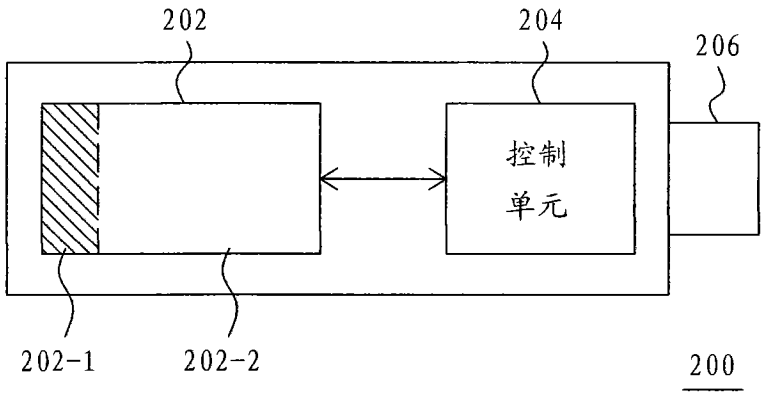

202
204
206
控制
单元
202-1
202-2
200

图 2

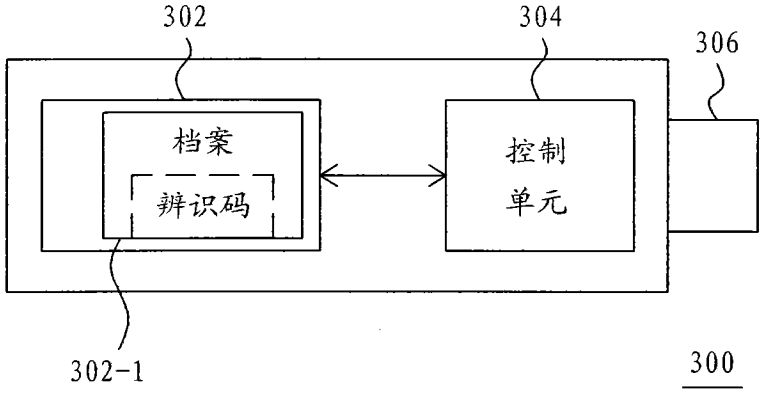

302
304
306
档案
辨识码
控制
单元
302-1
300

图 3

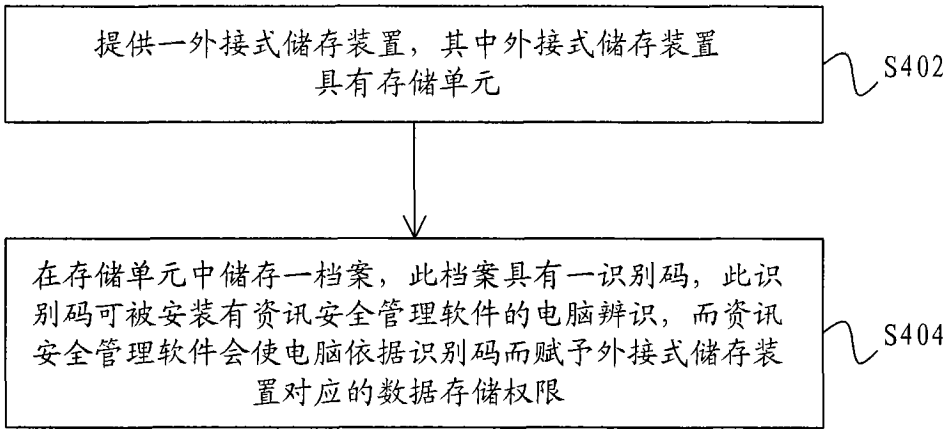

提供一外接式储存装置，其中外接式储存装置具有存储单元
S402
在存储单元中储存一档案，此档案具有一识别码，此识别码可被安装有资讯安全管理软件的电脑辨识，而资讯安全管理软件会使电脑依据识别码而赋予外接式储存装置对应的数据存储权限
S404

图 4

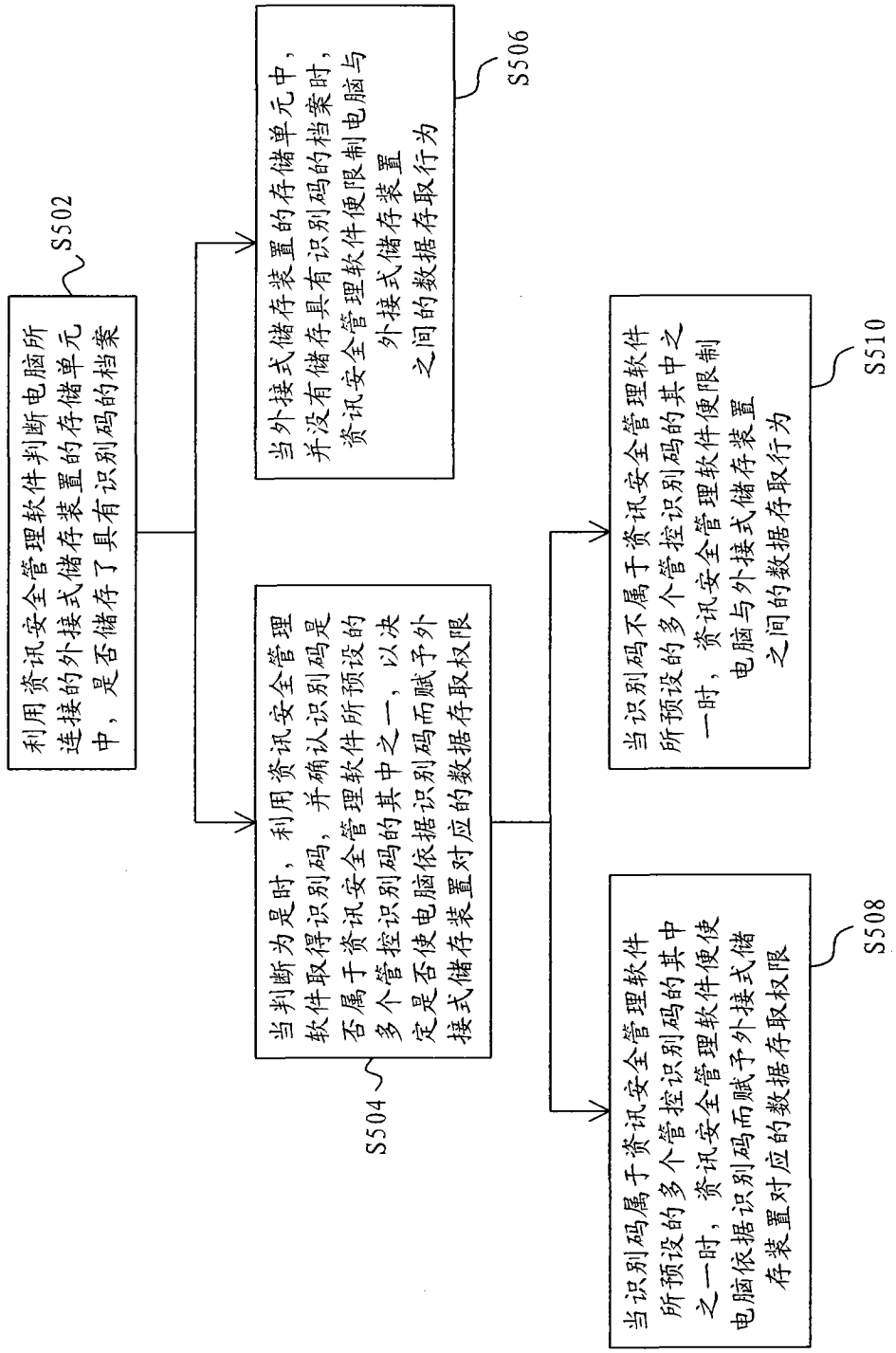

利用资讯安全管理软件判断电脑所连接的外接式储存装置的存储单元中，是否储存了具有识别码的档案
S502
当判断为是时，利用资讯安全管理软件取得识别码，并确认识别码是否属于资讯安全管理软件所预设的多个管控识别码的其中之一，以决定是否使电脑依据识别码而赋予外接式储存装置对应的数据存取权限
S504
当外接式储存装置的存储单元中，并没有储存具有识别码的档案时，资讯安全管理软件使限制电脑与外接式储存装置之间的数据存取行为
S506
当识别码属于资讯安全管理软件所预设的多个管控识别码的其中之一时，资讯安全管理软件使电脑依据识别码而赋予外接式储存装置对应的数据存取权限
S508
当识别码不属于资讯安全管理软件所预设的多个管控识别码的其中之一时，资讯安全管理软件使限制电脑与外接式储存装置之间的数据存取行为
S510

图 5