[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 12/14 (2006.01)
G06F 21/00 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200610002196.3

[45] 授权公告日 2009 年 4 月 8 日

[11] 授权公告号 CN 100476764C

[22] 申请日 2006.1.18
[21] 申请号 200610002196.3
[73] 专利权人 神盾股份有限公司
地址 台湾省台北市
[72] 发明人 周正三 张哲玮
[56] 参考文献
CN1624667A 2005.6.8
CN1696960A 2005.11.16
CN1281608A 2001.1.24
CN1359210A 2002.7.17
US6957337B1 2005.10.18
审查员 丛 珊

[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 任默闻

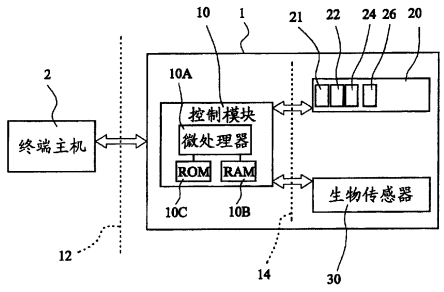
权利要求书 4 页 说明书 13 页 附图 4 页

[54] 发明名称

一种储存装置及其储存数据的保护方法

[57] 摘要

一种储存装置及其储存数据的保护方法，所述储存装置基本包含连接至终端主机的一控制模块以及连接至控制模块的一生物传感器及一储存模块。终端主机执行一生物辨识应用程序，以通知控制模块控制生物传感器读取使用者的一待辨识生物数据，并对比待辨识生物数据与储存装置中的模板生物数据是否吻合。对比吻合后，主机执行一主机乱码产生程序以产生并回传一组主机乱码至控制模块。控制模块利用储存于其中的一装置乱码产生程序产生一组装置乱码，并对比装置与主机乱码是否吻合，并依据吻合结果使主机能存取该储存装置的一数据保护单元。本发明既撷取了独立装置的优点，又能防止被破解，且不需要增加成本。



1. 一种储存装置，用以与一终端主机连接，该终端主机用以执行一生物辨识应用程序以及一主机乱码产生程序，其特征在于，所述储存装置包含:

一主机接口，用以与所述终端主机连接;

一控制模块，其连接至所述主机接口，并包含一微处理器、一随机存取存储器及一只读存储器，所述随机存取存储器作为数据处理时的工作存储器，而所述只读存储器储存有使所述储存装置工作的固件以及一装置乱码产生程序;

一生物传感器，其连接至所述控制模块，用以感测一使用者的一待辨识生物数据;

一数据保护单元，其连接至所述控制模块，并用以储存一待保护数据;及

一储存模块，其连接至所述控制模块，用以储存一模板生物数据;

其中:

所述模板生物数据是通过所述控制模块的微处理器被上传至所述终端主机;

在所述生物辨识应用程序的引导下，所述控制模块控制生物传感器读取使用者的待辨识生物数据，并将该待辨识生物数据传送至终端主机中;

所述终端主机利用生物辨识应用程序处理并对比待辨识生物数据与模板生物数据，并判断两者是否吻合，并在吻合时利用主机乱码产生程序依据一随时更新的乱码程序金钥来产生一组主机乱码，并将该主机乱码回传至微处理器中;且

该微处理器利用所述装置乱码产生程序依据随时更新的乱码程序金钥来产生一组装置乱码，并在对比这组装置乱码与这组主机乱码吻合时，使所述数据保护单元致能以供终端主机存取，否则使该数据保护单元禁能以防止终端主机存取。

2. 如权利要求 1 所述的储存装置，其特征在于，所述数据保护单元为储存模块中的一保密区块。

3. 如权利要求 1 所述的储存装置，其特征在于，所述数据保护单元为一外接存储器，其通过一存储器扩充插槽连接至所述控制模块。

4. 如权利要求 3 所述的储存装置，其特征在于，所述外接存储器被插入所述存储器扩充插槽后，所述控制模块将该外接存储器规划为单一扩充保密区块，用以储存待保护数据。

5. 如权利要求 1 所述的储存装置，其特征在于，所述数据保护单元为一大容量储存单元，其通过一储存接口扩充插槽而连接至所述控制模块。

6. 如权利要求 5 所述的储存装置，其特征在于，所述大容量储存单元还通过一加/解密芯片而连接至所述控制模块，用以加/解密进出该大容量储存单元的数据。

7. 如权利要求 1 所述的储存装置，其特征在于，所述生物辨识应用程序及所述主机乱码产生程序储存于所述储存模块的一应用程序区块中。

8. 如权利要求 7 所述的储存装置，其特征在于，所述应用程序区块被模拟成一光盘储存装置，藉以使连接至所述储存装置的终端主机自动执行生物辨识应用程序及主机乱码产生程序。

9. 如权利要求 1 所述的储存装置，其特征在于，所述主机乱码产生程序与装置乱码产生程序具有相同的程序逻辑。

10. 如权利要求 1 所述的储存装置，其特征在于，所述模板生物数据及随时更新的乱码程序金钥储存于所述储存模块的一隐藏区块中。

11. 如权利要求 1 所述的储存装置，其特征在于，所述随时更新的乱码程序金钥储存于所述储存模块中，且该随时更新的乱码程序金钥是通过所述控制模块的微处理器被上传至终端主机。

12. 如权利要求 1 所述的储存装置，其特征在于，所述随时更新的乱码程序金钥由所述生物辨识应用程序所产生。

13. 如权利要求 1 所述的储存装置，其特征在于，所述随时更新的乱码程序金钥由所述生物辨识应用程序依据待辨识生物数据所产生。

14. 如权利要求 1 所述的储存装置，其特征在于，所述随时更新的乱码程序金钥由所述生物辨识应用程序依据待辨识生物数据及一数学运算所产生。

15. 一种储存装置的储存数据的保护方法，其特征在于，包含以下步骤：

连接所述储存装置与一终端主机；

在终端主机执行一生物辨识应用程序；

将储存于所述储存装置的一模板生物数据传送至所述终端主机；

引导一使用者使用该储存装置的一生物传感器，以使该生物传感器撷取该使用者的一待辨识生物数据，并将该待辨识生物数据传送至所述终端主机；

利用生物辨识应用程序处理并对比所述待辨识生物数据与所述模板生物数据，并判断两者是否吻合，并在吻合时利用一主机乱码产生程序依据一随时更新的乱码程序金钥来产生一组主机乱码，并将该主机乱码回传至所述储存装置中；及

在所述储存装置中，利用一装置乱码产生程序依据所述随时更新的乱码程序金钥来产生一组装置乱码，并在对比这组装置乱码与这组主机乱码吻合时，使所述储存装置的一数据保护单元致能以供终端主机存取，否则使该数据保护单元禁能以防止终端主机存取。

16. 如权利要求 15 所述的储存装置的储存数据的保护方法，其特征在于，所述储存模块的一应用程序区块被模拟成一光盘储存装置，且其中储存有所述生物辨识应用程序及所述主机乱码产生程序，藉以使连接至所述储存装置的终端主机自动执行该生物辨识应用程序及该主机乱码产生程序。

17. 如权利要求 15 所述的储存装置的储存数据的保护方法，其特征在于，更包含以下步骤：将储存于所述储存装置的随时更新的乱码程序金钥传

送至终端主机。

18. 如权利要求 15 所述的储存装置的储存数据的保护方法，其特征在于，更包含以下步骤：利用所述生物辨识应用程序产生随时更新的乱码程序金钥。

19. 如权利要求 15 所述的储存装置的储存数据的保护方法，其特征在于，更包含以下步骤：利用所述生物辨识应用程序依据待辨识生物数据产生随时更新的乱码程序金钥。

20. 如权利要求 15 所述的储存装置的储存数据的保护方法，其特征在于，更包含以下步骤：利用所述生物辨识应用程序依据待辨识生物数据及一数学运算产生随时更新的乱码程序金钥。

一种储存装置及其储存数据的保护方法

技术领域

本发明有关于一种储存装置及其储存数据的保护方法，特别是有关于一种含指纹传感器的储存装置及其储存数据的保护方法。本发明也关联至部分发明人的下述专利:（a）中国发明专利申请案号200310116995.X，申请日为2003年12月5日，发明名称为“含指纹传感器的存储器储存装置及其储存数据的保护方法”;（b）中国发明专利申请案号 200410038204.0，申请日为2004年5月13日，发明名称为“含生物辨识的可携式加密储存装置及其储存数据的保护方法”；及（c）中国台湾发明专利申请案号094101590，申请日为2005年1月19日,发明名称为“一种储存装置及其储存数据的保护方法”。

背景技术

传统上，代表个人身份的表示方式，最简单莫过于证件，诸如身份证、驾驶执照等等，其上贴附有个人的照片及文字与数字记载。然而身份证件的仿冒太容易了，也因此造成许多犯罪行为。

更进一步的改良方法是利用磁条卡片记录个人的数据，同样的，科技的进步使得磁条卡片很容易被破解。

最新的方法是采用芯片卡的保密方式来保护个人数据。基本上，关于存储器芯片对个人数据的保密方面，最常使用方式是采用密码保护的方式。然而，使用密码来保护个人数据，不但具有使用者容易忘记密码的麻烦，更有着密码遭人破解的危险性。

同时，上述代表个人身份的装置（除了芯片卡外），都仅能执行单一功能，而无法将多重应用整合于单一装置中。

因此，美国专利公开第2003/0110389 A1号公报揭露一种类似于固态存

储器随身碟的个人身份电子装置，其内含已经加密的个人数据，可以直接连接于计算机系统而使用。然而，此个人身份电子装置同样也需要密码的设定才能开启，面临前述的问题。解决这一问题的最佳方法是利用个人特有的生物特征，譬如指纹、声纹、笔迹、眼睛虹膜等生物辨识方法，来提供较为完整且有效的数据保护方式。其优点为生物特征是随身携带且不需记忆，更无法被盗取，特别是结合指纹的生物特征保护方法，不仅严密，且使用相当方便。

近年来，更因为芯片式指纹传感器的发明，使得在轻薄短小的电子产品中整合指纹读取装置不再是不可行的技术，相关技术内容可参见本案其中一个发明人周正三的下述专利：1. 中国发明专利申请案号 02105960.8，申请日为 2002 年 4 月 10 日，发明名称为“电容式指纹读取芯片”，公开号为 1450489；2. 中国发明专利申请案号 02123058.7，申请日为 2002 年 6 月 13 日，发明名称为“压力式指纹读取芯片及其制造方法”，公开号为 1464471；3. 中国发明专利申请案号 02124906.7，申请日为 2002 年 6 月 25 日，发明名称为“温度传感器及其运用该温度传感器的指纹辨识芯片”，公开号为 1463674；及 4. 中国发明专利申请案号 02132054.3，申请日为 2002 年 09 月 10 日，发明名称为“电容式压力微感测元及其应用的指纹读取芯片结构”，公开号为 1482440。这也开拓了一种崭新的个人化储存媒体的保护方式。

早在二十年前美国专利第 4,582,985 号公报便已经揭露一种储存媒体的保护方法，其中利用指纹认证的方式来保护储存于个人身份卡片装置中的个人数据。在指纹辨识程序通过之后，储存于卡片装置中的受保护数据才得以输出以供进行后续的处理或认证程序。此种装置的尺寸相同于目前通用的信用卡，其主要包含一指纹传感器、影像处理与辨识模块、以及储存存储器，而成为一种完全独立的指纹辨识装置（也即指纹撷取及辨识都是在同一装置内执行）。

中国专利 CN1302018A 揭露一种通过指纹辨识来控制数据储存装置的

读写权的方法。然而，此专利并无明确地揭露此储存装置的格式及接口。

同样的，欧洲专利 EP124079A1 公报同样揭露相同于前述美国专利第4,582,985号公报的数据保护理念，但不同的是其沟通接口为供SD卡接口使用的金手指设计。此外，EP124079A1 专利的存储器装置具有一指纹辨识模块，且其数据保护概念相同于CN1302018A专利，除了EP124079A1专利的沟通接口是供SD卡接口使用的金手指构造以外。同样的，美国专利公开号US2001/0023375 A1也揭露一种用以通过指纹辨识来保护储存于硬盘或快闪盘的数据的方式。

世界专利 WO 02/42887A2 公报揭露一种相同于前述美国专利第4,582,985号公报及欧洲专利EP124079A1公报的数据保护理念，但不同的是，通过 USB 接口执行与终端系统的沟通，这一装置近似目前市场上流行的闪存，不同的是内含独立的指纹处理及辨识模块。

美国专利公开第 2003/005337 号公报揭露了相同于前述美国专利第4,582,985号公报及欧洲专利EP124079A1公报的数据保护理念，同时也相同于世界专利WO 02/42887A2公报所揭露利用USB作为沟通的接口。然而，其同样为一种独立式指纹辨识装置。

英国专利第GB2387933号公报也揭露几乎完全相同于WO 02/42887A2公报及美国专利公开第2003/005337号公报的理念及装置设计，其为一独立的指纹辨识装置。

至此，上述含有指纹辨识装置的发明，除了美国专利第4,582,985号公报揭露应用于个人身份证件代表外，其余都仅作为数据的保护，并无涵盖这一应用及功能。

此外，上述的含指纹辨识装置的可携式储存装置的基本要求，就是能让使用者能将此储存装置连接至不同的计算机系统以供使用。然而，上述已知技术含指纹辨识功能的储存装置设计，即使使用 USB 接口，仍需要在计算机系统上事先安装指纹应用程序，以让计算机系统能提供人机接口供使用

者方便使用。传统的作法是提供一光盘，以供使用者安装指纹应用程序，才能让整个储存装置可以方便使用。在此情况下，在每一台计算机系统的第一次设定中，使用者除了要携带可携式储存装置以外，还要携带光盘才能在其它计算机系统中使用此储存装置。

总之，上述已知技术的目的是提供一种用以通过指纹辨认来保护所储存的数据的储存装置。当使用此装置时，使用者必须事先安装指纹应用软件于终端系统中。因此，储存装置的指纹应用程序无法在各种不同计算机中方便地达到随插即用的效果。

至此，前述的已知技术有一共同的特色，也就是提供一独立的指纹辨识装置，内部包含指纹传感器、指纹图像处理及辨识IC。这样的设计优点为，或许不需要安装指纹应用程序于终端系统端而提供了热插拔的使用方便性，但却衍生出另一重要问题，那就是价格昂贵，因为必须增加一指纹图像处理及辨识 IC 及其配套设计的成本，通常该 IC 为 32 位的精简指令集计算机（Reduced Instruction Set Computer，RISC）或数字信号处理器（Digital Signal Processor，DSP），才能快速进行指纹辨识。因此，传统的具有指纹传感器的可携式储存装置具有高成本的缺点。

为解决高成本的问题，最佳方式是利用终端系统的微处理器执行指纹图像处理及辨识，便可以有效降低成本。但是目前已知技术对于这一方法并无明确揭露及提出解决方案。

因为如果要将指纹图像处理及辨识的工作由储存装置执行移转到终端系统的微处理器执行，则该发明装置必须要有自动下载指纹应用程序（包含指纹图像处理、辨识及加解密功能等等）于终端系统的功能，才能达到热插拔的功能，以及在任何终端系统都可以使用的方便性。这样的解决方案也是上述已知技术没有提供的。

为此，本案发明人在上述（a）至（c）专利中揭露了一种自动执行（AutoRun）指纹辨识及应用程序于终端系统的设计，将储存装置作切割成

几个区域，并将其中一个区域模拟成 CD-ROM（让终端系统认知到 CD-ROM 装置），而储存于该区域的指纹辨识及应用程序便可以被自动执行。解决已知技术高成本（需要独立辨识装置）或者需要事先在计算机上安装指纹辨识软件的方法。

在这一些发明案中，指纹影像的处理及对比都是在终端系统进行，当完成对比后再通过特殊指令（special command）通知储存装置开放读写的权限。

这样的设计仍有一些缺点，那就是如果有人能在终端主机拦截到该特殊指令，则有可能不需要指纹对比而破解了储存装置的安全性。

延续上述的发明，本案发明人将更进一步提供一种储存数据的保护方法，可以完全保护本发明储存装置在终端系统操作时不会被撷取到开启储存装置的钥匙。

发明内容

有鉴于此，本发明的主要目的就是提供一种储存装置及其储存数据的保护方法，所述储存装置与一终端主机连接，并通过与该终端主机的共同作用，可以在不大幅增加储存装置的成本下，来提供含指纹传感器的储存装置的有效数据保护方式。

本发明的另一目的是提供一种储存装置及其储存数据的保护方法，其能避免终端主机控制储存装置开启的特殊指令被拦截而丧失数据保护的功能。

为达成上述目的，本发明提供一种储存装置，用以与一终端主机连接，该终端主机用以执行一生物辨识应用程序以及一主机乱码产生程序。所述储存装置基本上包含：一主机接口，用以与所述终端主机连接；一控制模块，其连接至所述主机接口，并包含一微处理器、一随机存取存储器（RAM）及一只读存储器（ROM），所述 RAM 作为数据处理时的工作存储器，而所述 ROM 储存有使该储存装置工作的固件以及一装置乱码产生程序；一生物传

感器，其连接至所述控制模块，用以感测一使用者的一待辨识生物数据；一数据保护单元，其连接至所述控制模块，并用以储存一待保护数据；及一储存模块，其连接至所述控制模块，用以储存一模板生物数据。该模板生物数据是通过所述控制模块的微处理器被上传至所述终端主机。在生物辨识应用程序的引导下，所述控制模块控制生物传感器读取使用者的该待辨识生物数据，并将该待辨识生物数据传送至终端主机中。该终端主机利用该生物辨识应用程序处理并对比该待辨识生物数据与模板生物数据，并判断两者是否吻合，并在吻合时利用主机乱码产生程序依据一随时更新的乱码程序金钥来产生一组主机乱码，并将该主机乱码回传至微处理器中。该微处理器利用该装置乱码产生程序依据随时更新的乱码程序金钥来产生一组装置乱码，并在对比这组装置乱码与这组主机乱码吻合时，使数据保护单元致能（enable）以供终端主机存取，否则使数据保护单元禁能（disable）以防止终端主机存取。

为达成上述目的，本发明也提供一种储存装置的储存数据的保护方法，基本上包含以下步骤：连接储存装置与一终端主机；在终端主机执行一生物辨识应用程序；将储存于储存装置的一模板生物数据传送至终端主机；引导一使用者使用储存装置的一生物传感器，以使该生物传感器撷取该使用者的一待辨识生物数据，并将该待辨识生物数据传送至终端主机；利用生物辨识应用程序处理并对比待辨识生物数据与模板生物数据，并判断两者是否吻合，并在吻合时利用一主机乱码产生程序依据一随时更新的乱码程序金钥来产生一组主机乱码，并将该主机乱码回传至储存装置中；及在该储存装置中利用一装置乱码产生程序依据随时更新的乱码程序金钥来产生一组装置乱码，并在对比这组装置乱码与这组主机乱码吻合时，使该储存装置的一数据保护单元致能以供终端主机存取，否则使该数据保护单元禁能以防止该终端主机存取。

通过本发明的上述装置与方法，由于复杂的生物数据的对比动作是在

终端主机中执行，所以储存装置本身不需要高阶的微处理器。此外，生物数据对比成功后，终端主机所送出的信号并非是单纯用以开启待保护数据的信号，而是一组变化多端的信号，即使被拦截到，也不怕待保护数据外露。这是因为最后的数据保护单元的致能与禁能是在控制模块中进行的，且控制模块的对比数据是两组变化多端的乱码，只有在两组乱码对比成功后，才能开启数据保密单元的管理权限，因此能有效防止被破解。乱码的对比相当简单，可以利用譬如 8051 处理器的微处理器便可以处理，使本发明因而撷取了独立装置的优点也不需要增加成本。

附图说明

图 1 显示依本发明第一实施例的储存装置与一终端主机的连接状态示意图。

图 2 显示依本发明第二实施例的储存装置与一终端主机的连接状态示意图。

图 3 显示依本发明第三实施例的储存装置与一终端主机的连接状态示意图。

图 4 显示依本发明第四实施例的储存装置的保护方法的流程图。

主要组件符号说明:

1~储存装置	2~终端主机
10~控制模块	10A~微处理器
10B~随机存取存储器（RAM）	10C~只读存储器（ROM）
12~主机接口	16~储存接口
20~储存模块	21~应用程序区块
22~公用区块	24~保密区块/数据保护单元
26~隐藏区块	30~生物传感器
40~存储器扩充插槽	50~外接存储器/数据保护单元
60~加/解密芯片	70~储存接口扩充插槽

80~大容量储存单元/数据保护单元 210-310~方法步骤

具体实施方式

图 1 显示依本发明第一实施例的储存装置与一终端主机的连接状态示意图。如图 1 所示，本实施例的一种储存装置 1 是用以与一终端主机 2 连接。该终端主机 2 用以执行一生物辨识应用程序以及一主机乱码产生程序。所述生物辨识应用程序以及所述主机乱码产生程序可以预先储存于储存装置 1 中，再通过自动执行（Auto Run）的方式而使终端主机 2 自动执行。

储存装置 1 基本上包含一主机接口 12、一控制模块 10、一生物传感器 30、一储存模块 20 及一数据保护单元 24。主机接口 12 用以与终端主机 2 连接。主机接口 12 可以是一通用串行总线（USB）接口、一 PCMCIA 接口、SATA 接口、一 PCI 高速（PCI EXPRESS）接口或一 IEEE 1394 接口或其它标准接口。控制模块 10 连接至主机接口 12，并包含一微处理器 10A、一随机存取存储器（RAM）10B 及一只读存储器（ROM）10C。所述 RAM 10B 作为数据处理时的工作存储器，而所述 ROM 10C 储存有使储存装置 1 工作的固件（firmware）以及一装置乱码产生程序。所述微处理器 10A、RAM 10B 及 ROM 10C 可以整合在单一芯片中而成为单芯片设计。因此，控制模块 10 的任务是与终端主机 2 沟通，同时管理储存模块 20 及生物传感器 30。

所述生物传感器 30 连接至控制模块 10，用以感测一使用者的一待辨识生物数据。该生物传感器 30 可以感测使用者的生物数据，譬如指纹、虹膜、声音、笔迹或其它生物数据等，且生物传感器 30 可以是一面积型指纹传感器、一滑动式指纹传感器、一声纹传感器、一虹膜传感器或一脸型传感器或其它类型生物传感器，以下仅以指纹传感器来作说明。

所述储存模块 20 连接至控制模块 10，用以储存一模板生物数据以及一随时更新的乱码程序金钥（该乱码程序金钥也可以每次使用时由指纹应用程序产生，而不需要事先储存于储存模块 20 中）。所谓的模板生物数据，就是储存装置 1 的拥有者在第一次使用此装置时，在其中所留下的第一次的生物

数据，此指纹数据是用以作为与后续指纹数据对比的基准。储存模块 20 可以是一种存储器模块或一硬盘装置，存储器模块为选自于一非挥发性存储器，例如一闪存、一可编程只读存储器（PROM）、一只读存储器、或一电可擦除只读存储器（EEPROM）等等。硬盘装置具有相同的切割。在本实施例中，储存模块 20 被分割为一应用程序区块 21、一公用区块 22、一保密区块 24 及一隐藏区块 26。保密区块 24 是作为数据保护单元用，因此其也是连接至控制模块 10，并用以储存一待保护数据。在终端主机 2 要自动执行生物辨识应用程序及主机乱码产生程序的情况下，该生物辨识应用程序及该主机乱码产生程序可以储存于应用程序区块 21 中。此外，该应用程序区块 21 是被模拟成一光盘储存装置，藉以使连接至该储存装置 1 的终端主机 2 自动执行该生物辨识应用程序及该主机乱码产生程序。该主机乱码产生程序与该装置乱码产生程序具有相同的程序逻辑，也就是，根据同一乱码程序金钥可以产生相同的乱码。公用区块 22（可以选择性的设计存在或不存在）可以储存公用程序及数据，藉以让使用者在不用通过生物辨识程序之前即可使用该公用程序及数据。在一实施例中，模板生物数据及随时更新的乱码程序金钥储存于隐藏区块 26 中。在另一实施例中，乱码程序金钥不预先储存于隐藏区块 26，而是每次使用时由指纹应用程序根据指纹特征（取自于待辨识生物数据）产生，抑或结合指纹特征及一数学运算产生。所谓随时更新的乱码程序金钥是指供给主机及装置乱码产生程序的起始值，该随时更新的乱码程序金钥在每次主机乱码与装置乱码对比成功后会被更新，以确保这一储存装置无法被轻易破解。

当储存装置 1 连接至终端主机 2 时，模板生物数据及随时更新的乱码程序金钥是通过控制模块 10 的微处理器 10A 被上传至终端主机 2。然后，在终端主机 2 所执行的生物辨识应用程序的引导下，控制模块 10 控制生物传感器 30 读取使用者的待辨识生物数据，并将该待辨识生物数据传送至终端主机 2 中。接着，终端主机 2 利用生物辨识应用程序处理，并对比待辨识

生物数据与模板生物数据，并判断两者是否实质上吻合，并在实质上吻合时利用主机乱码产生程序依据随时更新的乱码程序金钥来产生一组主机乱码，并将主机乱码回传至微处理器 10A 中，主机乱码回传的方式可以是直接传送，或者加密后回传（到微处理器 10A 中也必需要先解密再对比），也或者结合通信协议一起传送（例如与 USB 控制器沟通的通信协议）。如果乱码程序金钥每次使用时由指纹应用程序产生的情况下，其回传方式也可以如同上述主机乱码的回传方式。值得注意的是，生物数据的对比方式可以用图形对比、特征点对比等方式。然后，微处理器 10A 利用装置乱码产生程序依据随时更新的乱码程序金钥来产生一组装置乱码，并在对比这组装置乱码与这组主机乱码实质上吻合时，使数据保护单元 24 致能以供终端主机 2 存取，否则使数据保护单元 24 禁能以防止终端主机 2 存取。

图 2 显示依本发明第二实施例的储存装置与一终端主机的连接状态示意图。如图 2 所示，本实施例类似于第一实施例，不同之处在于本实施例的储存装置 1 更包含一存储器扩充插槽 40，其与控制模块 10 电连接，用以与一外接存储器 50 电连接，藉以增加该储存装置 1 的存储器容量。该存储器扩充插槽 40 实质上用以扩充本发明装置的存储器的容量，抑或通过将本装置视为一外接存储器 50 的读取器（memory reader），该外接存储器譬如 CF 卡、智能型媒体（smart media）、记忆棒（memory stick）或其它标准接口的外接存储器、或硬盘（特别是一寸或更小的硬盘，又称微型硬盘（microdrive））。外接存储器 50 是在这组装置乱码与这组主机乱码实质上相符时被致能以供终端主机 2 存取。在外接存储器 50 被插入存储器扩充插槽 40 后，控制模块 10 将该外接存储器规划为单一扩充保密区块，用以储存额外的待保护数据。

此外，图 2 中的外接存储器 50，也可以单独作为数据保护单元，其通过存储器扩充插槽 40 连接至控制模块 10。在此情况下，储存模块 20 的保密区块 24 可以省略。在外接存储器 50 被插入存储器扩充插槽 40 后，控制模

块 10 将该外接存储器规划为单一扩充保密区块，用以储存待保护数据。

图 3 显示依本发明第三实施例的储存装置与一终端主机的连接状态示意图。如图 3 所示，本实施例类似于第一实施例，不同之处在于本实施例的储存装置 1 更包含一储存接口扩充插槽 70，其用以将一大容量储存单元 80 电连接至控制模块 10，藉以为该储存装置 1 提供一储存容量。加/解密芯片 60 通过一储存接口 16 连接至控制模块 10。储存接口扩充插槽 70 连接至加/解密芯片 60。大容量储存单元 80 通过储存接口扩充插槽 70 及加/解密芯片 60 而连接至控制模块 10。该大容量储存单元 80 是在装置乱码与主机乱码实质上相符时被致能以供终端主机 2 存取。进出该大容量储存单元 80 的数据可以通过加/解密芯片 60 进行加/解密。该大容量储存单元 80 的一个实施例为磁性硬盘，特别是 3.5 寸、2.5 寸或其它尺寸的硬盘；该大容量储存单元 80 的另一个实施例为 CD-R/RW 及 DVD-R/RW 及任何规格的光盘装置。储存接口 16 及储存接口扩充插槽 70 在本实施例中为 IDE 接口，然而也可以是 SCSI 接口、Serial ATA 接口、一 Compact Flash（CF） 接口、一 PCMCIA 接口或 IEEE 1284 接口或者其它标准的接口。

此外，图 3 中的大容量储存单元 80，也可以单独作为数据保护单元。在此情况下，储存模块 20 的保密区块 24 可以省略。数据保护单元是通过储存接口扩充插槽 70 而连接至控制模块 10。此外，该大容量储存单元 80 更通过加/解密芯片 60 而连接至控制模块 10，用以加/解密进出该大容量储存单元 80 的数据。

图 4 显示依本发明第四实施例的储存装置的保护方法的流程图。如图 4 所示，本发明的储存装置 1 的储存装置的保护方法包含以下步骤。

首先，在储存装置 1 被插入至终端主机 2 后，通过储存装置 1 的主机接口 12 来连接储存装置 1 与终端主机 2。然后，终端主机 2 执行生物辨识应用程序，如步骤 210 所示。接着生物辨识应用程序自动判断该储存装置 1 是否第一次被使用，如果是，则询问使用者是否登录其指纹数据，如步骤 220

所示。若使用者选择登录数据，则如步骤225开始登录指纹。在此情况下，生物传感器30感测使用者的指纹数据，如步骤235所示，然后提取指纹模板，如步骤245所示，接着以金钥加密模板，如步骤255所示。然后，将指纹模板数据储存在隐藏区块26中。

当生物辨识应用程序中侦测到隐藏区块26中储存有指纹模板数据，该储存装置1将储存于该储存装置1的一模板生物数据以及一随时更新的乱码程序金钥传送至终端主机2，如步骤230与240所示。然后，生物辨识应用程序引导使用者使用该储存装置1的一生物传感器30，以使该生物传感器30撷取该使用者的一待辨识生物数据，并将该待辨识生物数据传送至终端主机2，如步骤250所示。接着，利用生物辨识应用程序处理并对比待辨识生物数据与模板生物数据，并判断两者是否实质上吻合，如步骤260所示。若两者实质上不吻合时，则询问使用者是否继续对比，如步骤270所示。若使用者不继续对比，则整个流程结束。若使用者要继续对比，则回到步骤250。若两者实质上吻合，利用主机乱码产生程序依据随时更新的乱码程序金钥来产生一组主机乱码，并将该主机乱码回传至储存装置1中，如步骤280所示。

然后，在储存装置1中利用一装置乱码产生程序依据该随时更新的乱码程序金钥来产生一组装置乱码，如步骤290所示。接着，对比这组装置乱码与这组主机乱码是否实质上吻合，如步骤300所示。当这组装置乱码与这组主机乱码实质上吻合时，使储存装置1的一数据保护单元24/50/80致能以供终端主机2存取，如步骤310所示。否则使该数据保护单元24/50/80禁能以防止终端主机2存取而结束。

值得注意的是，本方法可以应用在上述三个实施例，因此详细内容在此不再详述。

通过本发明的上述装置与方法，由于复杂的生物数据的对比动作是终端主机中执行，所以储存装置本身不需高阶的微处理器。此外，生物数据对比成功后，终端主机所送出的信号并非是单纯用以开启待保护数据的信号，

而是一组变化多端的信号，即使被拦截到，也不怕待保护数据外露。此是因为最后的数据保护单元的致能与禁能是在控制模块中进行的，且控制模块的对比数据是两组变化多端的乱码，只有在两组乱码对比成功后，才能开启数据保密单元的管理权限，因此能有效防止被破解。乱码的对比相当简单，可以利用譬如 8051 处理器的微处理器便可以处理，使本发明因而撷取了独立装置的优点也不需要增加成本。

在较佳实施例的详细说明中所提出的具体实施例仅用以方便说明本发明的技术内容，而非将本发明狭义地限制于上述实施例，在不超出本发明的精神及申请专利范围的情况，所做的种种变化实施，都属于本发明的范围。

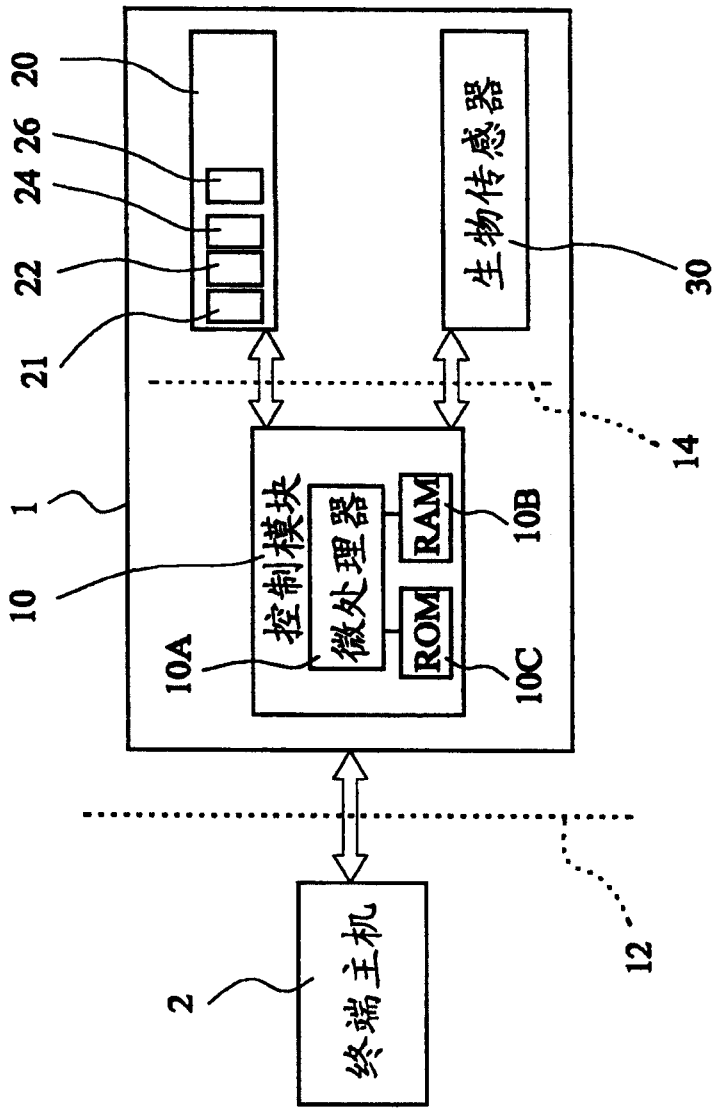

20
24 26
22
21
1
10
生物传感器
30
14
控制模块
微处理器
RAM
ROM
10A
10B
10C
12
2
终端主机

图 1

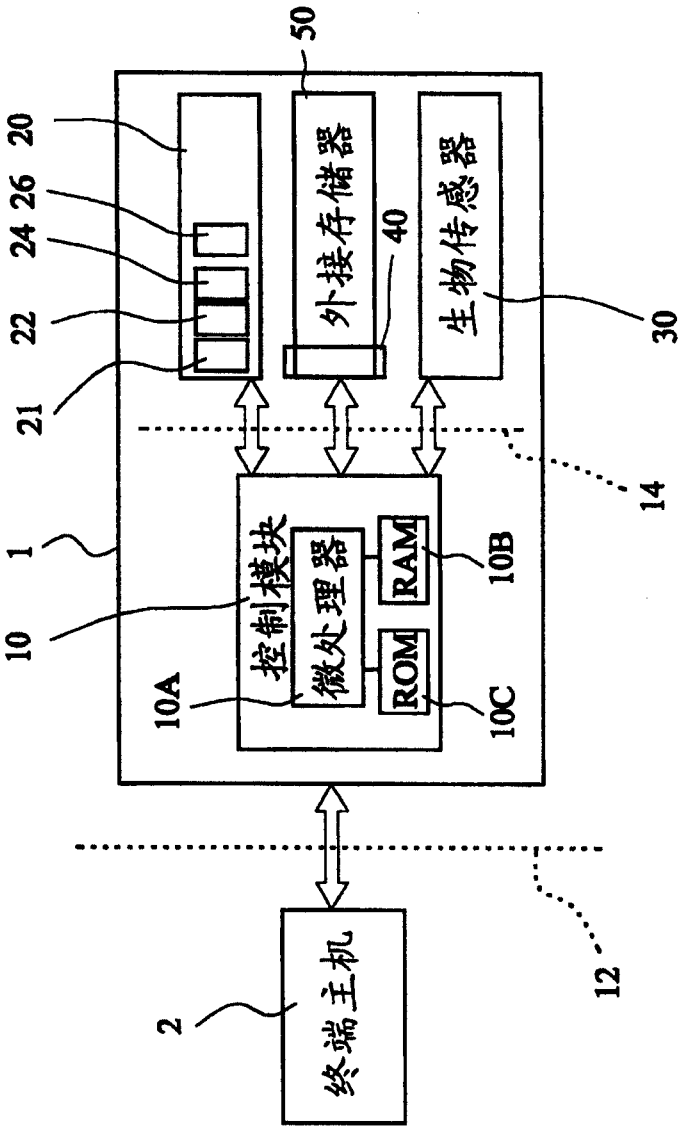

50
20
24 26
22
21
外接存储器
40
生物传感器
30
1
10
控制模块
微处理器
RAM
10B
ROM
10C
10A
14
12
2
终端主机

图 2

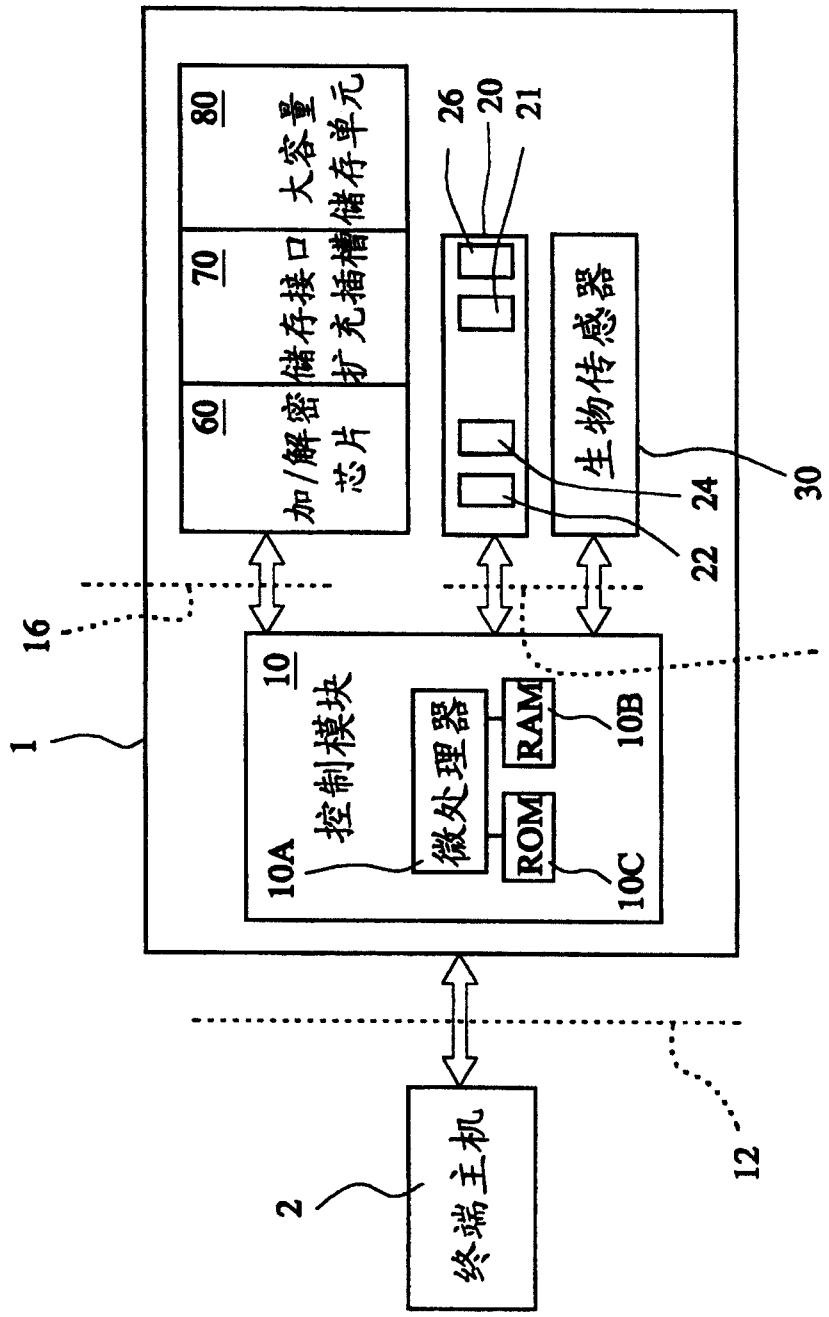

1
16
10
控制模块
10A
微处理器
ROM
10C
RAM
10B
14
60
加/解密
芯片
70
储存接口
扩充插槽
80
大容量
储存单元
26
20
21
22
24
生物传感器
30
2
终端主机
12

图 3

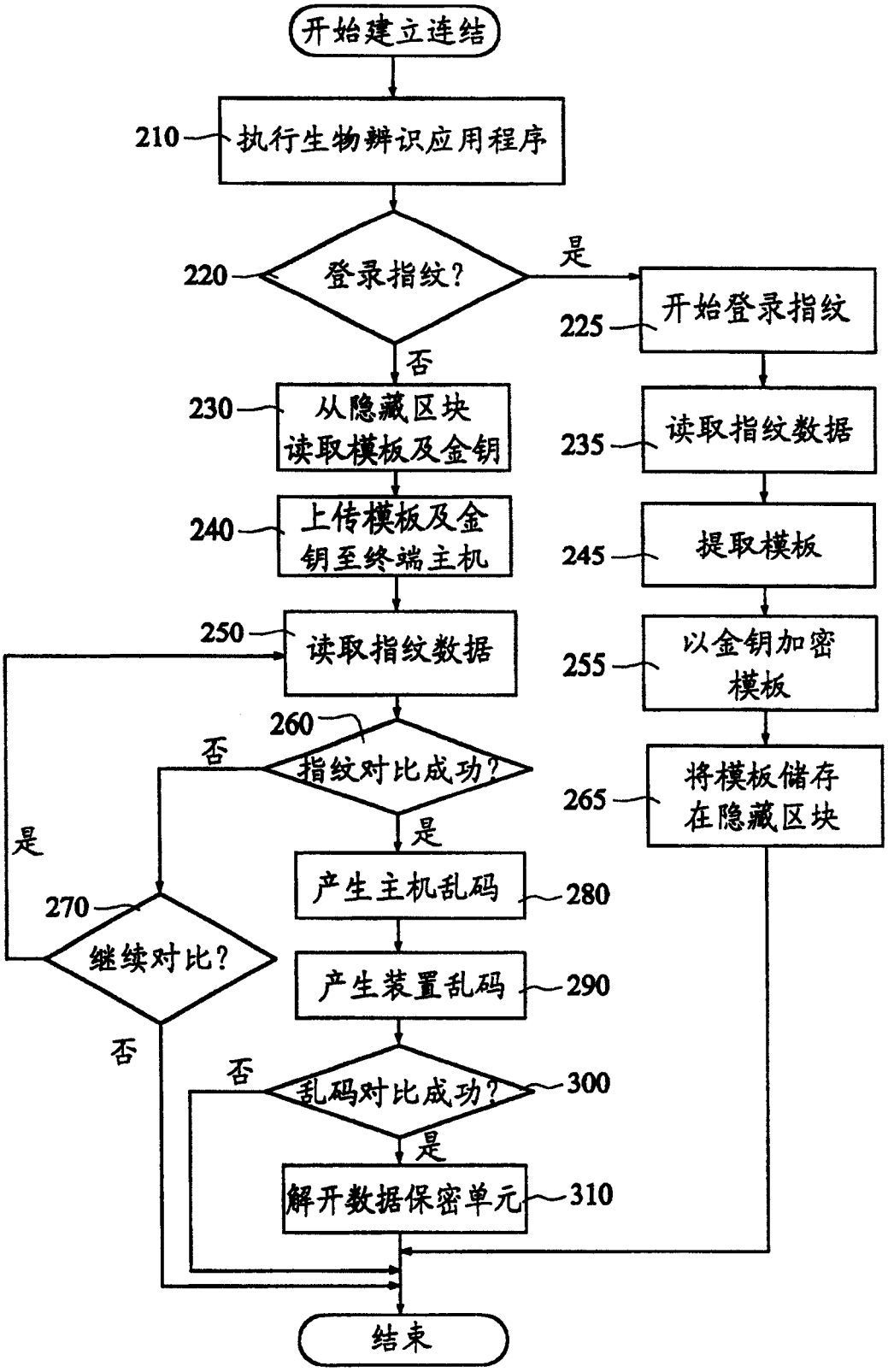

开始建立连结
210
执行生物辨识应用程序
220
登录指纹?
是
225
开始登录指纹
否
230
从隐藏区块
读取模板及金钥
235
读取指纹数据
240
上传模板及金
钥至终端主机
245
提取模板
250
读取指纹数据
255
以金钥加密
模板
260
否
指纹对比成功?
265
将模板储存
在隐藏区块
是
是
产生主机乱码
280
270
继续对比?
产生装置乱码
290
否
否
乱码对比成功?
300
是
解开数据保密单元
310
结束

图 4