

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06F 12/14 (2006.01)

G06K 9/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 200310116995.X

[45] 授权公告日 2006 年 11 月 8 日

[11] 授权公告号 CN 1284090C

[22] 申请日 2003.12.5

[21] 申请号 200310116995.X

[71] 专利权人 瀚群科技股份有限公司

地址 台湾省台北县

共同专利权人 鑫创科技股份有限公司

祥群科技股份有限公司

[72] 发明人 邱立国 陈明舜 古茂源 陈盈苍

周正三

审查员 吴 敏

[74] 专利代理机构 北京三友知识产权代理有限公司

代理人 王占梅

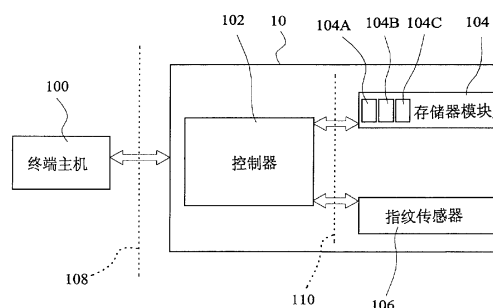
权利要求书 4 页 说明书 11 页 附图 5 页

[54] 发明名称

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

[57] 摘要

本发明揭示了一种含指纹传感器的存储器储存装置，其基本包含连接至一终端主机的一主机接口、连接至主机接口的一控制器、以及连接至控制器的一指纹传感器及一存储器模块。控制器与终端主机相连接，并令终端主机将适合于终端主机的驱动程序及应用程序从存储器模块加载安装至终端主机中。终端主机通过这两程序接收来自使用者的一指令，以通知控制器控制指纹传感器读取使用者的一待辨识指纹数据。终端主机利用应用程序处理待辨识指纹数据及储存于该存储器模块的模板指纹数据，并判断两者是否实质上吻合，更依据吻合结果使终端主机能存取存储器模块的一特定区块。



1、一种含指纹传感器的存储器储存装置，用以与一终端主机连接，其特征是包含：

一主机接口，用以与所述终端主机连接；

一控制器，连接至所述主机接口，通过所述主机接口而与所述终端主机相连接，以便将一模板指纹数据传输至所述终端主机中；

一指纹传感器，连接至所述控制器，用以感测一使用者的一待辨识指纹数据；及

一存储器模块，连接至所述控制器，所述存储器模块被分割为：

一公用区块，用以储存多个应用程序；

一保密区块，用以储存一待保护数据；及

一隐藏区块，用以储存所述模板指纹数据，其中：

所述终端主机执行其中一个所述应用程序，并通过所述应用程序接收来自所述使用者的一指令，以通知所述控制器控制所述指纹传感器读取所述使用者的所述待辨识指纹数据，并将所述待辨识指纹数据传送至所述终端主机中；以及利用所述应用程序处理所述待辨识指纹数据及所述模板指纹数据，并判断两者是否实质上吻合，并于实质上吻合时使所述保密区块能够供所述终端主机存取，否则使所述保密区块禁止以防止所述终端主机存取。

2、根据权利要求1所述的含指纹传感器的存储器储存装置，其特征是：所述隐藏区块还储存有一加/解密金钥，并通过所述控制器传输至所述终端主机中。

3、根据权利要求2所述的含指纹传感器的存储器储存装置，其特征是：所述终端主机的所述应用程序通过所述加/解密金钥来将从所述保密区块存取的所述待保护数据予以加密/解密。

4、根据权利要求1所述的含指纹传感器的存储器储存装置，其特征是：所

述主机接口是一通用串行总线接口、一 PCMCIA 接口、一 PCI 高速接口或一 IEEE 1394 接口。

5、根据权利要求 1 所述的含指纹传感器的存储器储存装置，其特征是：所述指纹传感器是面积型指纹传感器或滑动式指纹传感器。

6、根据权利要求 1 所述的含指纹传感器的存储器储存装置，其特征是：还包含：

一扩充插槽，与所述控制器电连接，用以与一外接存储器电连接，藉以增加所述存储器储存装置的存储器容量。

7、根据权利要求 6 所述的含指纹传感器的存储器储存装置，其特征是：所述外接存储器为单一扩充保密区块，用以储存额外的待保护数据。

8、一种含指纹传感器的存储器储存装置，用以与一终端主机连接，其特征是包含：

一主机接口，用以与所述终端主机连接；

一控制器，连接至所述主机接口，通过所述主机接口与所述终端主机相连；

一指纹传感器，连接至所述控制器，用以感测一授权使用者的一模板指纹数据；及

一存储器模块，连接至所述控制器，所述存储器模块被分割为：

一公用区块，用以储存多个应用程序；

一保密区块，用以储存一待保护数据；及

一隐藏区块，用以储存一模板指纹数据，其中：

所述终端主机执行其中一个所述应用程序，并通过所述应用程序接收来自所述授权使用者的一指令，以通知所述控制器控制所述指纹传感器读取所述授权使用者的所述模板指纹数据，并将所述模板指纹数据传送至所述终端主机中；以及利用所述应用程序处理所述模板指纹数据，并将处理过的所述模板指纹数据传输至所述隐藏区块中储存。

9、根据权利要求 8 所述的含指纹传感器的存储器储存装置，其特征是：所

述隐藏区块还储存有一加/解密金钥，并通过所述控制器传输至所述终端主机中。

10、根据权利要求 9 所述的含指纹传感器的存储器储存装置，其特征是：所述终端主机的所述应用程序通过所述加/解密金钥来将从所述保密区块存取的所述待保护数据予以加密/解密。

11、根据权利要求 8 所述的含指纹传感器的存储器储存装置，其特征是：所述主机接口是一通用串行总线接口、一 PCMCIA 接口、一 PCI 高速接口或一 IEEE 1394 接口。

12、根据权利要求 8 所述的含指纹传感器的存储器储存装置，其特征是：所述指纹传感器是面积型指纹传感器或滑动式指纹传感器。

13、根据权利要求 8 所述的含指纹传感器的存储器储存装置，其特征是：还包含：

一扩充插槽，与所述控制器电连接，用以与一外接存储器电连接，藉以增加所述存储器储存装置的存储器容量。

14、根据权利要求 13 所述的含指纹传感器的存储器储存装置，其特征是：所述外接存储器为单一扩充保密区块，用以储存额外的待保护数据。

15、一种含指纹传感器的存储器储存装置的储存数据的保护方法，所述存储器储存装置包含一主机接口，用以与一终端主机连接；一控制器，连接至所述主机接口；一指纹传感器，连接至所述控制器，用以感测一授权使用者的一模板指纹数据；及一存储器模块，连接至所述控制器，所述存储器模块被分割为：一公用区块，用以储存多个应用程序；一保密区块，用以储存一待保护数据；及一隐藏区块，其中，在将所述存储器储存装置与一终端主机电连接之后，所述保护方法的特征是包含以下步骤：

所述控制器通过所述主机接口而与所述终端主机相连，并令所述终端主机执行适合于所述终端主机的其中一个所述应用程序；以及

进入一指纹登入模式或一指纹认证模式，

于所述指纹登入模式中:

所述终端主机通知所述控制器控制所述指纹传感器读取所述授权使用者的所述模板指纹数据, 并将所述模板指纹数据传送至所述终端主机中; 及

所述终端主机利用所述应用程序处理所述模板指纹数据, 并将处理过的所述模板指纹数据传输至所述隐藏区块中储存; 以及

于所述指纹认证模式中:

所述控制器将所述模板指纹数据传输至所述终端主机中;

所述终端主机通知所述控制器控制所述指纹传感器读取一使用者的一待辨识指纹数据, 并将所述待辨识指纹数据传送至所述终端主机中; 以及

所述终端主机利用所述应用程序处理所述待辨识指纹数据及所述模板指纹数据, 并判断两者是否实质上吻合, 并于实质上吻合时使所述保密区块能够供所述终端主机存取, 否则使所述保密区块禁止以防止所述终端主机存取。

16、根据权利要求 15 所述的含指纹传感器的存储器储存装置的储存数据的保护方法, 其特征是: 所述隐藏区块更用以储存一加/解密金钥, 且所述控制器将所述加/解密金钥传输至所述终端主机中, 而所述终端主机的所述应用程序是通过所述加/解密金钥来将从所述保密区块存取的所述待保护数据予以加密/解密。

17、根据权利要求 15 所述的含指纹传感器的存储器储存装置的储存数据的保护方法, 其中, 所述存储器储存装置还包含一扩充插槽, 与所述控制器电连接, 用以与一外接存储器电连接, 藉以增加所述存储器储存装置的存储器容量, 其特征在于, 所述保护方法还包含以下步骤:

在所述外接存储器被插入所述扩充插槽后, 所述控制器将所述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。

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

技术领域

本发明涉及一种存储器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存储器储存装置及其储存数据的保护方法。

背景技术

传统上，关于个人数据保密的作法，最常使用的是采用密码保护的方式来达成。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，更有密码遭人破解的危险性。因此，关于个人特有的生物数据，譬如指纹、声纹、笔迹、眼睛虹膜等生物辨识方法，已经逐渐被发展来提供较为完整且有效的数据保护方式。其优点为生物特征随身携带且不须存储，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，使得轻薄短小的电子产品整合指纹辨识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序号 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]；2、中国发明专利申请案序号 02123058.7，申请日为 2002 年 06 月 13 日，发明名称为[压力式指纹读取芯片及其制造方法]；3、中国发明专利申请案序号 02124906.7，申请日为 2002 年 07 月 12 日，发明名称为[温差感测元及其应用于指纹热像读取]；及 4、中国发明专利申请案序号 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]。这也开拓了一种崭新的个人化应用，亦即个人随身的电子产品附带指纹辨识的功能。

特别是在储存媒体的保护方面，更是结合生物辨识方法的重要发展项目，

例如：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分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。此种装置的横向尺寸相同于目前通用的信用卡，其主要包含一指纹传感器、影像处理及辨识模块及储存存储器，为一完全独立的指纹辨识装置（亦即指纹撷取及辨识都是在同一装置内执行）。即使其应用标的为防止例如个人信用卡等的仿冒，然而，这种装置的价格昂贵，例如除了指纹传感器外，影像处理及辨识模块需要高阶的微处理器例如 32 位(bits) 的 RISC 处理器或 DSP 芯片，使得这一种独立辨识装置不易推广。

美国专利第 6, 213, 403 号公报揭露一种具有指纹传感器的储存装置，其乃利用 PCMCIA 的接口来与计算机连接，相同的，此一装置的理念几乎相同于美国专利第 4, 582, 985 号公报所揭露的，为一独立的指纹辨识装置（亦即指纹撷取及辨识都是在同一装置内执行），通过指纹的认证才能开启该储存装置中的数据。不同指出是利用一标准的 PCMCIA 接口执行。同时，PCMCIA 装置是将整个卡片塞入计算机插槽中，为此该发明必须通过复杂的机构设计方能将指纹感测装置暴露于外以方便使用，这都会增加机构的不稳定性及成本。

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，美国专利第 6, 213, 403 号公报的数据保护理念，不同之处是其沟通接口为较不常见的金手指设计，同样的为一独立式指纹辨识模块。

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，美国专利第 6, 213, 403 号公报，欧洲专利 EP124079A1 公报的数据保护理念，不同之处是藉由 USB 接口执行与终端系统的沟通，此一装置近似目前市场上流行的闪存硬盘，不同处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，美国专利第 6, 213, 403 号公报，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。相同的为一独立式指纹辨识装置。

英国专利第 GB2387933 号公报亦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，为一独立的指纹辨识装置(亦即指纹撷取及辨识都是在同一装置内执行)。

至此，前述的习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)或数字讯号处理器(Digital Signal Processor, DSP)，才能快速进行指纹辨识。处理器的成本通常随着其运算速度与处理能力的增加而增加，上述的 RISC 及/或 DSP 的最小成本也要在美金 10 元以上。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，最佳方式为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。但是目前习知技术对于此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，方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习知技术没有提供的。

或者如美国专利公开第 2003/005337 号公报揭露的，可以将指纹处理及辨识软件安装于终端系统上，这样的设计使得使用者便无法在不同终端系统使用，或者需要费时费力的安装软件。传统的作法是提供一光盘片，以供使用者分别安装储存装置中的存储器的驱动程序，以及指纹传感器的驱动程序，才能让整个储存装置可以开始使用。于此情况下，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，还要携带光盘片才能在其它计算机系统中使用此储存装置。虽然可以通过网络下载驱动程序，但这并不是完美的作法，因为有些计算机不一定都能连上网络。

因此，本发明将提供一种含指纹感测装置的储存装置及其储存数据的保护方法，特色有二。一为利用终端系统的处理器做指纹处理及辨识，可以大幅降低装置的硬件成本，达到普及的目的。二为提供一完全自动下载指纹应用程序的功能，藉由整合 USB 控制器的固件(firmware)，指纹辨识及处理软件，以及相关 AP(application program)在一起，本发明的装置除了完全不需要在终端系统安装任何驱动程序或辨识软件，便可以完全热插拔的使用于各种操作系统的终端系统，特别是计算机装置，而且支持各种语言操作系统。

同时，本装置存储器所储存的个人数据，是以加密方式存录，即使将该存储器拔除也无法撷取出正确的格式及内容。

发明内容

有鉴于此，本发明的主要目的就是提供一种含指纹传感器的存储器储存装置，该存储器储存装置是与一终端主机连接，并藉由与该终端主机的共同作用，可以在不大幅增加该储存装置的成本下，来提供含指纹传感器的存储器储存装置。

本发明的另一目的是提供一种含指纹传感器的存储器储存装置，其能对一终端主机隐藏其指纹传感器及存储器，用以简化该终端主机的控制方式。

为达成上述目的，本发明提供一种含指纹传感器的存储器储存装置，用以与一终端主机连接，该存储器储存装置包含：一主机接口，用以与该终端主机连接；一控制器，连接至该主机接口；一指纹传感器，连接至该控制器，用以感测一使用者的一待辨识指纹数据；及一存储器模块，连接至该控制器。

控制器对存储器模块分割成多个磁盘。这种方法由控制器所完成，而非主机。对于主机，上述多个磁盘中的每一个对于主机而言都是真正的磁盘，而非

逻辑磁盘。而且，一个磁盘还可以被分割多个区域。一些区域可被所有终端用户自由存取，另一些则只能由指定用户通过识别后进行存取。据此，可以实现数据保护或保密功能。控制器对该存储器模块分割成三个区域包含：一公用区块，用以储存多个应用程序；一保密区块，用以储存一待保护数据；及一隐藏区块，用以储存一模板指纹数据及加密金钥。一旦存储器储存装置插入主机插槽，控制器在初始电源开启后，将信息区块读入控制器的 SRAM 内。根据装载入 SRAM 的信息区块数据，控制器将对主机发出的请求做出反应，对存储器模块进行配置，并将其视为逻辑磁盘。主机将读到存储器模块的公用区块的应用程序，而执行该程序于该主机中。该控制器将该模板指纹数据传输至该主机中。该主机通过该逻辑磁盘数据存取及该应用程序接收来自该使用者的一指令，以通知该控制器控制该指纹传感器读取该使用者的该待辨识指纹数据，并将该待辨识指纹数据传送至该主机中。该终端主机利用该应用程序处理该待辨识指纹数据及该模板指纹数据，并判断两者是否实质上吻合，并于实质上吻合时使该保密区块致能以供该终端主机存取，否则使该保密区块禁能以防止该终端主机存取。

该模板指纹数据的建立方式如下。该控制器通过该主机接口而与该终端主机沟通，并令该终端主机将适合于该终端主机的其中一个驱动程序及其中一个应用程序加载安装至该终端主机中。该终端主机通过该驱动程序及该应用程序接收来自一授权使用者的一指令，以通知该控制器控制该指纹传感器读取该授权使用者的该模板指纹数据，并将该模板指纹数据传送至该终端主机中。该终端主机利用该应用程序处理该模板指纹数据，并将处理过的该模板指纹数据传输至该隐藏区块中储存。

本发明的特色在于解决上述习知技术的两大问题。

一为本发明装置是利用终端系统的微处理器执行指纹图像处理及辨识，取代习知技术装置内含独立的指纹辨识微处理器，以大幅降低成本。

二为本发明装置虽然没有独立的指纹辨识微处理器，却可以自动下载指纹应用程序于终端系统使用，不需要人为的安装于终端系统中，使得本发明装置

得以随身携带，方便的使用于不同的终端系统。

为了让本发明的上述和其它目的、特征、和优点能更明显易懂，下文特举一较佳实施例，并配合附图，作详细说明。

附图说明

图 1 表示依本发明第一实施例的具有一指纹传感器的存储器储存装置与一终端主机的连接状态示意图。

图 2 表示具有指纹传感器的存储器储存装置的应用系统流程。

图 3 显示将本发明装置的存储器模块切割成不同独立区域的示意图。

图 4 表示依本发明第二实施例的具有一指纹传感器的存储器储存装置与一终端主机的连接状态示意图。

图 5 显示将本发明应用于一拇指盘的实体外观图。

图 6 显示将本发明应用于一拇指盘的实体分解图。

具体实施方式

如图 1 所示，其为本发明实施例含指纹传感器的存储器储存装置 10 的功能方块图。该装置 10 基本上包含一个控制器 102，一个存储器模块 104、一个指纹传感器 106 及一主机接口 108。在本实施例中主机接口为通用序列汇流排(USB)的接口，然而也可以是一 PCMCIA 接口、PCI 高速(PCI EXPRESS)接口或一 IEEE 1394 接口或者其它标准的接口。USB 接口 108 是与终端主机 100 连接，控制器 102 连接至主机接口，使得控制器 102 通过主机接口 108 而与终端主机 100 连接，并通过存储器接口 110 与存储器模块 104 连接。控制器 102 的任务是与终端主机 100 沟通，同时管理存储器模块 104 及指纹传感器 106。存储器模块 104 须包括至少一个用来储存数据的储存芯片或存储器，例如闪存、可编程只读存储器(PROM)、只读存储器(ROM)或可电性抹除可编程只读存储器(EEPROM)。存储器模块 104 被分割为：一公用区块 104A，用以储存包含一指纹应用程序在内的

至少一应用程序；一保密区块 104B，用以储存一待保护数据；及一隐藏区块 104C，用以储存至少一模板指纹数据，更可用以储存一加/解密金钥，而该控制器 102 更可将该加/解密金钥传输至该终端主机 100 中，使得终端主机 100 的应用程序是通过加/解密金钥来将从保密区块 104B 存取的待保护数据予以加密/解密。

指纹传感器 106 特别是上述其中一位发明人周正三的专利申请案中所提的电容式、温差感应式或压力式的指纹传感器。包含了用以感测静置于其上的手指指纹的面积型指纹传感器或用以感测滑动通过其上的手指指纹的滑动式指纹传感器。指纹传感器 106 受控制器 102 存取控制抓取实时的指纹数据使用。终端主机 100 将所抓取实时的指纹数据与先前的模板指纹数据做模板比对。所谓的模板指纹数据，就是存储器储存装置 10 的拥有者于第一次使用此装置时，在其中所留下的第一次的指纹数据，此指纹数据是用以作为与后续指纹数据比对的基准。因此，指纹传感器 106 是连接至该控制器 102，用以感测授权使用者的模板指纹数据，更可用以感测一使用者的一待辨识指纹数据来跟模板指纹数据比对。

如图 2 所示，本发明的存储器储存装置 10 在连接至终端主机 100 之后的储存数据的保护方法如下。首先，控制器 102 通过主机接口 108 而与终端主机 100 沟通，并令终端主机 100 将适合于终端主机 100 的操作系统的驱动程序及指纹应用程序加载安装至该终端主机 100 中，如步骤 210 所示。然后，于步骤 220，终端主机 100 上显示出一窗口供使用者选择或自动判定进入一指纹登入模式（步骤 225）或一指纹认证模式（步骤 230）。

若要进入指纹登入模式，则终端主机 100 通知控制器 102 控制指纹传感器 106 读取授权使用者的模板指纹数据，并将模板指纹数据传送至终端主机 100 中（步骤 235、245）。此时，终端主机 100 利用指纹应用程序处理模板指纹数据，并将处理过的模板指纹数据传输至隐藏区块 104C 中储存。或者，指纹应用程序可以利用金钥加密指纹模板数据（步骤 255），然后将加密过的模板指纹数据传

输至隐藏区块 104C 中储存(步骤 265)。

若要进入指纹认证模式,则控制器 102 自隐藏区块 104C 读取模板指纹数据(步骤 230),使模板指纹数据得以被传输至终端主机 100 中,然后以金钥解密指纹模板数据(步骤 240)。接着,终端主机 100 通知控制器 102 控制指纹传感器 106 读取使用者的待辨识指纹数据,并将待辨识指纹数据传送至终端主机 100 中(步骤 250)。然后,终端主机 100 利用应用程序处理待辨识指纹数据及模板指纹数据,并判断两者是否实质上吻合,并于实质上吻合时解开保密区块以使保密区块 104B 致能以供终端主机 100 存取(步骤 280),否则使保密区块 104B 禁能以防止终端主机 100 存取,或者询问使用者是否再继续比对来进行认证(步骤 270)。

为了更清楚说明本发明装置如何自动下载指纹应用程序于终端系统执行,本发明发明人的 3S 专利清楚的描述了本发明装置中控制器 102 如何管理存储器模块 104 以及位于存储器模块内的数据或程序,在此将该 3S 专利案列为参考数据(附件),以供查询。

简而言之,本发明装置所使用的控制器 102 管理存储器模块 104 的方法,是可以将该存储器模块切割成不同的独立区块以分别储存不同的数据,以本发明实施例而言,该存储器模块 104 是被切割成一公用区块 104A、一保密区块 104B 及一隐藏区块 104C。请参见图 3,其是为应用 3S 专利发明存储器管理方法,将本发明装置的存储器模块 104 切割成不同独立区域的说明。

如图 3 所示,本发明的存储器储存装置 10 中的控制器 102 将存储器模块 104 的逻辑空间 200 分割成三个完全独立区块,其中包含第 0 至 P 个逻辑区块的公用区块 104A、第 Q 至 M-1 个逻辑区块的保密区块 104B 以及第 M 个逻辑区块的隐藏区块 104C。分区信息是储存在特定的信息区块内。逻辑空间 200 是映像至实体空间 202,而实体空间 202 包含了信息区块及第 1 至 N 个实体区块。

当本发明装置与终端系统连接后,终端系统会将本装置视为一独立的磁盘 600,并且自动连接存储器模块 104 中的独立公用区块 104A,以在终端系统的

显示装置上显现出指纹应用程序的档案选项，并且由使用者选择以执行该指纹应用程序，例如出现一指纹登录画面。

当使用者执行完该公用区块 104A 的指纹应用程序后，控制器 102 会自动切换区块，由公用区块 104A 切换至保密区块 104B。相对应的，在终端系统显示装置上会出现画面的切换，亦即切换至受保护的保密区块 104B，以显示出该区块内受保护的数据，使使用者可以自由存取。

简而言之，使用本发明装置时，控制器 102 会先切换至公用区块自动下载指纹应用程序，待执行完指纹应用程序后再切换至保密区块。而这样的自动下载及画面切换的功能，也是因为本发明申请人的 3S 专利专有控制器 102 设计有存储器独立切割及管理的功能，而致使本发明装置可以有别于现有习知技术，藉由终端系统的微处理器作指纹的处理及识别，同时也兼顾自动下载含指纹应用程序在内的各种应用程序。

值得说明的是，本发明的公共区块的任何应用程序都是只读文件，无法作任何更动。

在本发明中，另外有一隐藏区块 104C，此区块需通过特殊程序直接与控制器 102 沟通，系统无从察觉此区块，隐藏区块 104C 的大小可根据设计调整。隐藏区块存放模板指纹数据、加密金钥、电子凭证...等私密数据。根据需要，亦可将隐藏区块的大小设置为零，这时，终端系统面对本装置所映像的磁盘 600 仅仅显现磁盘中保密区块 104B 及公用区块 104A 而已。

于本发明另一实施例中，如图 4 所示，存储器储存装置 10 除了包含类似于图 1 的控制器 102、存储器模块 104、指纹传感器 106 及主机接口 108 以外，可以更包含一存储器扩充插槽 103，该存储器扩充插槽 103 是实质上用以扩充本发明装置的存储器的容量，亦或藉由将本装置视为一外接存储器 105 的读取器 (memory reader)，该外接存储器譬如智能型媒体 (smart media) 或存储卡 (memory stick) 或其它标准接口的外接存储器。扩充插槽 103 是通过存储器接口 110 而与控制器 102 电连接，用以与一外接存储器 105 电连接，藉以增加存

存储器储存装置的存储器容量。当外接存储器 105 被插入扩充插槽 103 后, 控制器 102 将外接存储器 105 规划为单一扩充保密区块, 用以储存额外的待保护数据。如此一来本装置可以提供任何外接存储器 105 数据保护的方法。

以下再次参见图 1 与图 2 来说明本发明的应用系统流程。

首先, 存储器储存装置 10 插入主机 100 的插槽, 控制器 102 在初始电源开启后, 控制器 102 通过主机接口 108 而与主机 100 沟通, 控制器 102 将信息区块读入控制器的 SRAM 内。根据装载入 SRAM 的信息区块数据, 控制器将对主机发出的请求做出反应, 对存储器模块 104 进行配置, 并将其视为逻辑磁盘。主机 100 将读到存储器模块 104 的公用区块 104A 的应用程序并执行。此动作是由控制器 102 控制而自动执行, 使用者不需手动安装驱动程序与应用程序。

然后, 主机 100 通过直接执行应用程序并由应用程序接收来自授权使用者的一指令(可以用弹跳窗口的方式引导使用者进行), 以通知控制器 102 控制指纹传感器 106 读取授权使用者的模板指纹数据, 并将模板指纹数据传送至该主机 100 中。

接着, 主机 100 利用此应用程序处理此模板指纹数据, 并将处理过的模板指纹数据传输至隐藏区块 104C 中储存。然后, 使用者可以将私密数据储存到保密区块 104B 中。

当使用者将存储器储存装置 10 携带至另一台主机 100 中使用时, 控制器 102 通过主机接口 108 而与主机 100 交握沟通, 控制器 102 将对主机 100 发出的请求做出反应, 对存储器模块 104 进行配置, 并将其视为逻辑磁盘, 并将其中一个应用程序加载安装至主机 100 中执行。然后, 主机 100 的应用程序判断出存储器模块 104 的隐藏区块 104C 中已经储存有模板指纹数据, 或者控制器 102 将隐藏区块 104C 中已经储存有模板指纹数据的状况通知主机 100。于此情况下, 控制器 102 将模板指纹数据传输至主机 100 中。主机 100 通过直接执行应用程序并由应用程序接收来自使用者的一指令, 以通知控制器 102 控制指纹传感器 106 读取使用者的待辨识指纹数据, 并将待辨识指纹数据传送至主机 100

中。主机 100 利用应用程序处理待辨识指纹数据及模板指纹数据，并判断两者是否实质上吻合，并于实质上吻合时使保密区块 104B 致能以供主机 100 存取，否则使保密区块 104B 禁能以防止主机 100 存取。

为了更进一步保护存储器模块 104 的保密区块 104B 的私密数据，可以在隐藏区块 104C 中的加密金钥将对保密区块 104B 的私密数据做储存加/解密动作（由应用程序处理）。在控制器 102 控制下，加/解密金钥可以被传输至主机 100 中。藉此，主机 100 的应用程序就可以通过加/解密金钥来将从保密区块 104B 存取的待保护数据予以加密/解密处理。

为了表示本发明的可实施性，以下提供将本发明应用于拇指盘的实体外观图（图 5），以及实体分解图（图 6）以兹证明。

藉由本发明的上述构造，从计算机系统上所看到的联机装置，不再包含一个非挥发性存储器以及一个指纹传感器，所以不需要同时安装适用于该非挥发性存储器以及该指纹传感器的驱动程序，所以计算机系统不需多任务控制两个装置的运作。取而代之的是，从计算机系统上所看到的联机装置，仅有一个可携式储存装置，所以计算机系统仅需控制一个装置的运作。至于可携式储存装置内的非挥发性存储器与指纹传感器的运作，可以由控制器来控制。值得注意的是，本发明所指的控制器，是可以宽广地包含控制非挥发性存储器与指纹传感器的运作的其它组件，譬如只读存储器（ROM）、随机存取存储器（RAM）等。

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以下申请专利范围的情况，所做的种种变化实施，皆属于本发明的范围。

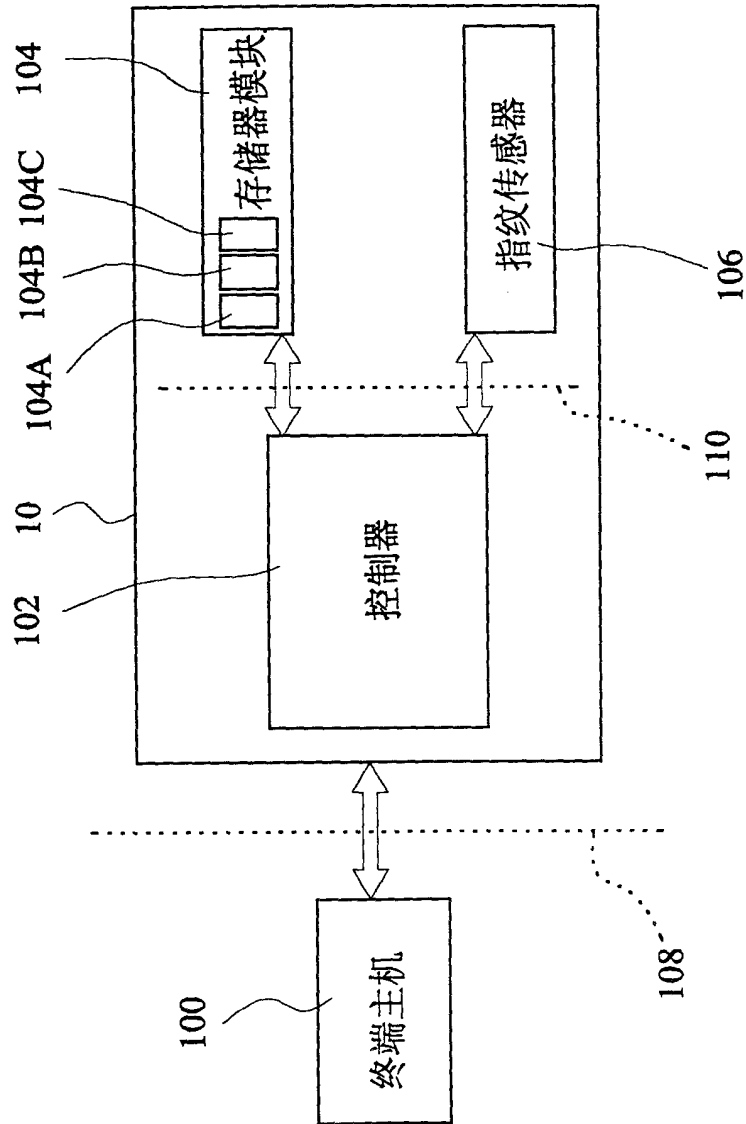


图 1

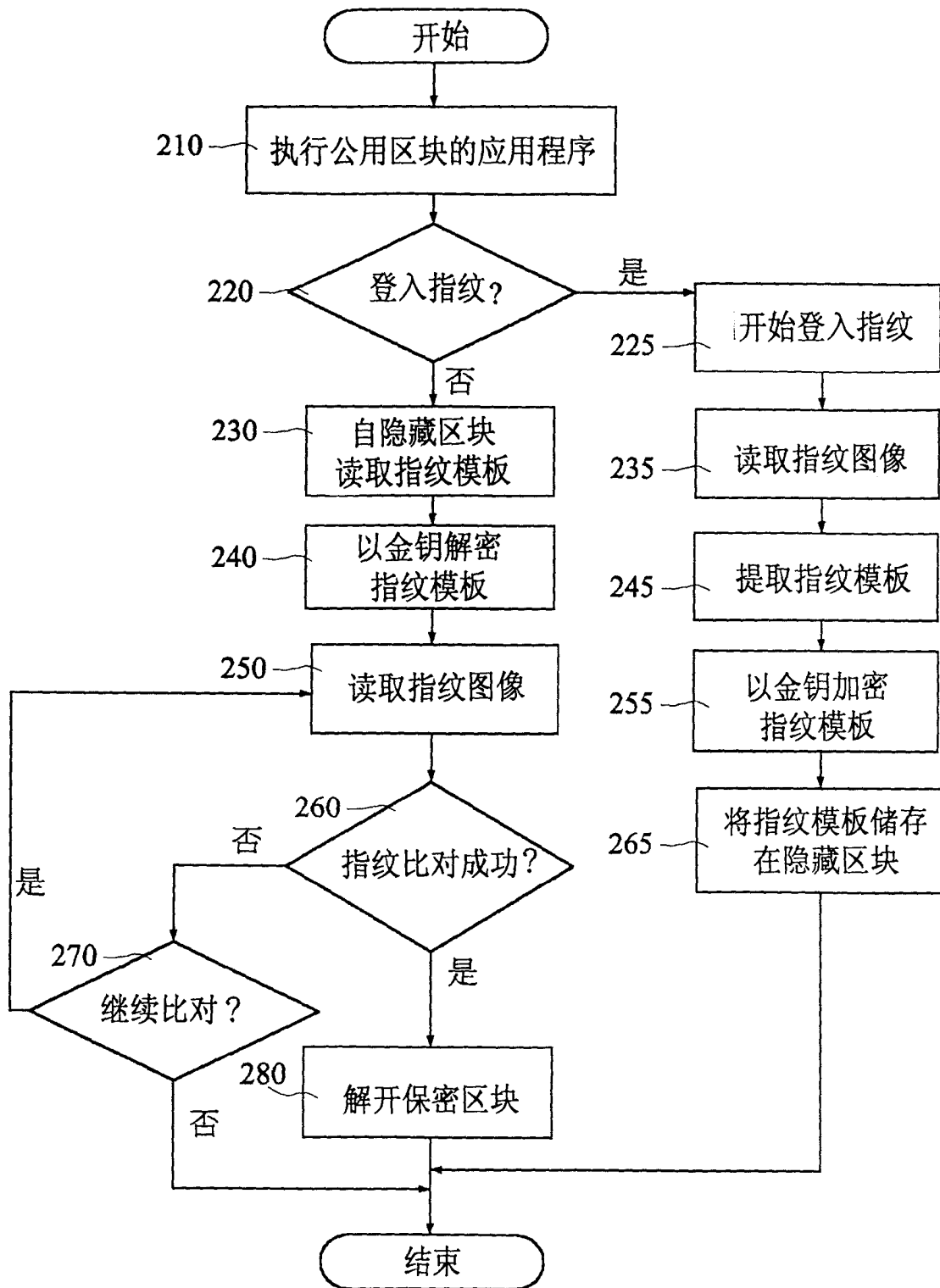
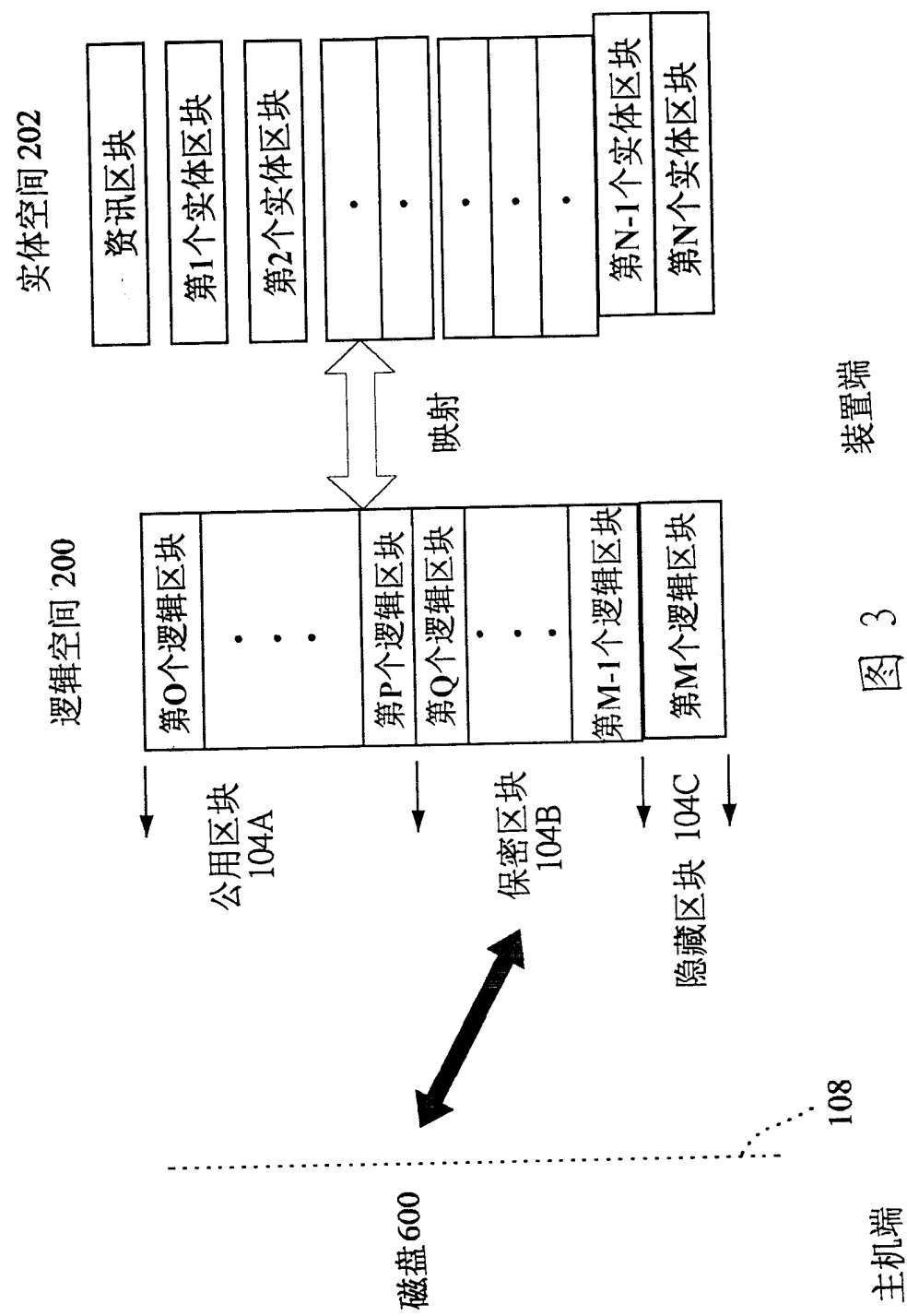


图 2



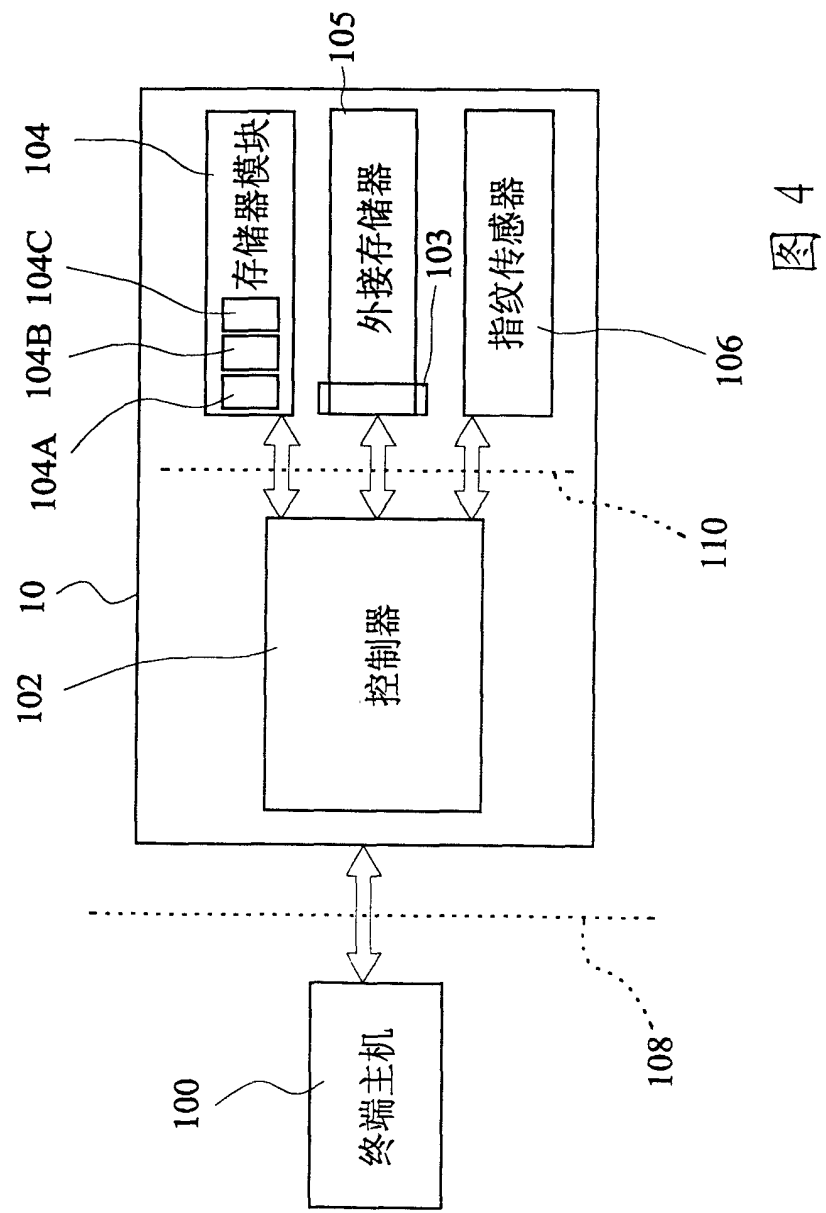


图 4

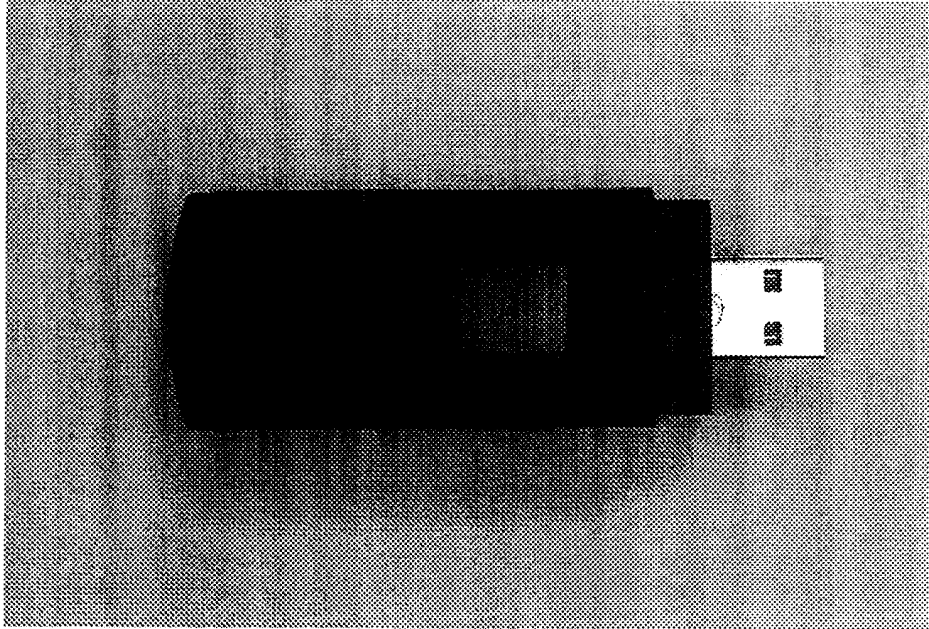


图 5

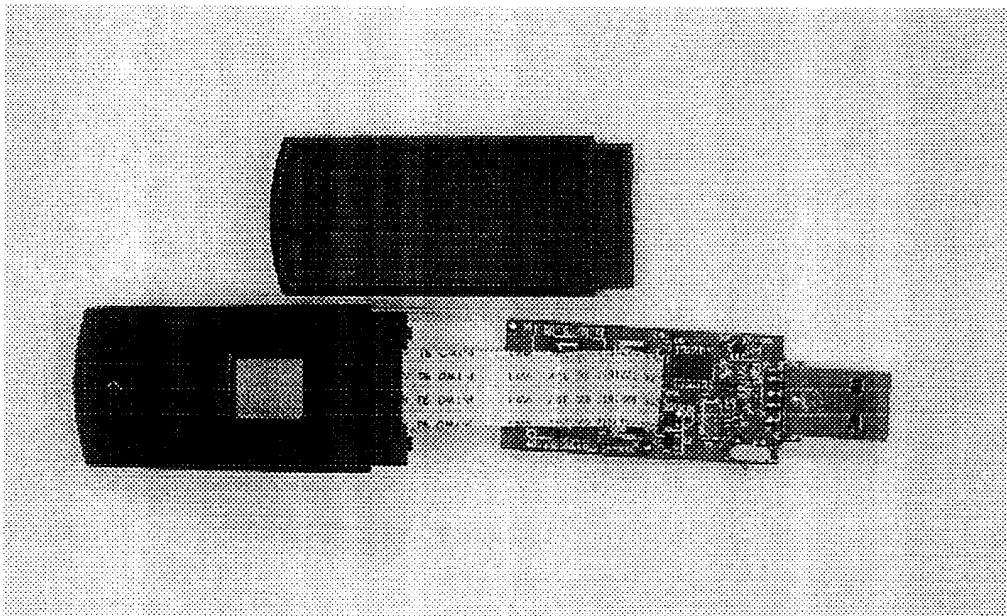


图 6