

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06K 9/00 (2006.01)

G07F 7/10 (2006.01)

G06F 15/16 (2006.01)

G09F 3/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 03121338.3

[45] 授权公告日 2007 年 5 月 30 日

[11] 授权公告号 CN 1319010C

[22] 申请日 2003.3.26 [21] 申请号 03121338.3

[73] 专利权人 祥群科技股份有限公司
地址 台湾省新竹科学工业园区

[72] 发明人 周正三

[56] 参考文献

- CN1290380A 2001.4.4
- US4720860A 1988.1.19
- WO02/48485A1 2002.6.20
- US5280527A 1994.1.18
- US4582985A 1986.4.15
- CN1341905A 2002.3.27
- CN2481807Y 2002.3.13

审查员 朱 骥

[74] 专利代理机构 北京三友知识产权代理有限公司
代理人 马娅佳

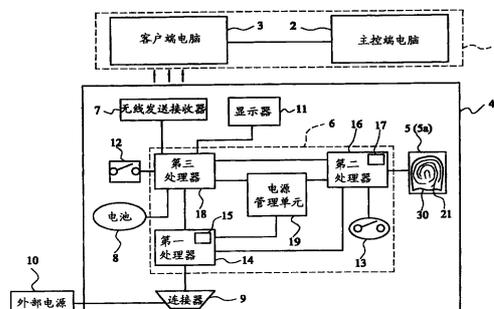
权利要求书 4 页 说明书 9 页 附图 2 页

[54] 发明名称

卡片式生物辨识装置及方法

[57] 摘要

一种卡片式生物辨识装置包含一生物感测器、一运算处理模组、一无线收发器及一可充电式电池。生物感测器用以读取持有者的生物资料。运算处理模组储存有乱码产生程式、个人资料及一笔授权生物资料，然后可接收并处理一笔待辨识生物资料，并于判断待辨识生物资料实质上符合授权生物资料后，透过乱码产生程式产生并输出一笔待辨识码。无线收发器输出个人资料至一主机系统，使主机系统依据储存于其中的对应个人资料的乱码产生程式产生一笔授权码，由比较授权码与待辨识码，即可判断待辨识持有者是否为授权持有者。



1. 一种卡片式生物辨识装置,用以辨识在一主机系统侧的一待辨识持有者是否为一授权持有者,该主机系统储存有该授权持有者的一笔个人资料及对应该个人资料的一乱码产生程式,该卡片式生物辨识装置包含:

一生物感测器,用以读取并输出该授权持有者的一笔授权生物资料以及该待辨识持有者的一笔待辨识生物资料:

一运算处理模组,仅供单次接收、处理并储存该乱码产生程式、该个人资料及该授权生物资料,然后可多次接收并处理该待辨识生物资料,并于判断该待辨识生物资料实质上符合该授权生物资料后,透过该乱码产生程式产生并输出一笔待辨识码:

一无线收发器,输出该个人资料至该主机系统,使该主机系统依据对应该个人资料的该乱码产生程式产生一笔授权码,由比较该授权码与该待辨识码,即可判断待辨识持有者是否为该授权持有者:及

一可充电式电池,用以提供该运算处理模组、该生物感测器及该无线收发器所需的电源。

2. 如权利要求1所述的卡片式生物辨识装置,其特征在于,该无线收发器更用以输出该笔待辨识码,使该主机系统依据该笔待辨识码及该笔授权码判断待辨识持有者是否为该授权持有者。

3. 如权利要求1所述的卡片式生物辨识装置,其特征在于,更包含:

一连接器,连接至该运算处理模组,透过该连接器可接收该个人资料及该乱码产生程式。

4. 如权利要求1所述的卡片式生物辨识装置,其特征在于,更包含:

一连接器,连接至该运算处理模组,透过该连接器可接收该个人资料及该乱码产生程式,且透过该连接器可接收一外部电源来对该可充电式电池充电。

5. 如权利要求1所述的卡片式生物辨识装置,其特征在于,更包含:

一显示器,连接至该运算处理模组,用以显示该笔待辨识码。

6. 如权利要求1所述的卡片式生物辨识装置, 其特征在于, 更包含:
一电源开关, 连接至该运算处理模组, 供该授权持有者及该待辨识持有者控制该可充电式电池提供该电源。

7. 如权利要求1所述的卡片式生物辨识装置, 其特征在于, 更包含:
一生物资料读取开关, 仅供单次开启以让该授权持有者输入该授权生物资料。

8. 如权利要求1所述的卡片式生物辨识装置, 其特征在于, 该运算处理模组包含:

一第一处理器, 其具有一第一记忆体, 该第一处理器是用以单次接收、处理与储存该乱码产生程式及该个人资料:

一第二处理器, 其具有一第二记忆体, 该第二处理器是与该第一处理器及该生物感测器连通, 用以单次接收、处理并储存该授权生物资料, 然后可多次接收并处理该待辨识生物资料, 并于判断该待辨识生物资料实质上符合该授权生物资料后, 促使该第一处理器输出该笔待辨识码;

一第三处理器, 与该第一处理器连通, 用以接收、处理并输出该个人资料及一笔待辨识码: 及

一电源管理单元, 连接至该第一处理器、该第二处理器及该第三处理器, 用以作电源管理。

9. 如权利要求1所述的卡片式生物辨识装置, 其特征在于, 该主机系统包含:

一主控端电脑, 储存有该乱码产生程式及该个人资料:

一客户端电脑, 与该主控端电脑连通, 作为与该卡片式生物辨识装置沟通的介面。

10. 如权利要求1所述的卡片式生物辨识装置, 其特征在于, 更包含一全像防伪标签。

11. 如权利要求1所述的卡片式生物辨识装置, 其特征在于, 该生物感测

器是为—指纹感测器、—声音感测器或—数位板。

12. 如权利要求1所述的卡片式生物辨识装置，其特征在于，该可充电式电池是为—高分子锂电池。

13. 如权利要求1所述的卡片式生物辨识装置，其特征在于，该生物感测器是为—一种晶片式指纹感测器。

14. 如权利要求13所述的卡片式生物辨识装置，其特征在于，该晶片式指纹感测器是为—一种二维式指纹感测器或—一维式指纹感测器。

15. 如权利要求1所述的卡片式生物辨识装置，其特征在于，该主机系统中的该乱码产生程式是与该运算处理模组中的该乱码产生程式同步产生该授权码与该待辨识码。

16. 如权利要求1所述的卡片式生物辨识装置，其特征在于，该无线收发器更用以接收来自该主机系统的沟通讯号。

17. 一种卡片式生物辨识方法，用以辨识在一主机系统侧的持有一卡片式生物辨识装置的一待辨识持有者是否为该卡片式生物辨识装置的一授权持有者，该主机系统与该卡片式生物辨识装置都储存有该授权持有者的一笔个人资料及对应该个人资料的一乱码产生程式，而该卡片式生物辨识装置储存有该授权持有者的一笔授权生物资料，该卡片式生物辨识方法包含以下步骤：

读取并输出该待辨识持有者的一笔待辨识生物资料至—运算处理模组：

以该运算处理模组处理并判断该待辨识生物资料是否与该授权生物资料实质上相符：

若该待辨识生物资料与该授权生物资料实质上相符，则由该运算处理模组依据储存于其中的该乱码产生程式产生一笔待辨识码：及

由该运算处理模组输出该个人资料至该主机系统，使该主机系统依据对应至该个人资料的该乱码产生程式产生一笔授权码，藉由比较该笔待辨识码及该笔授权码，即可判断该待辨识持有者是否为该授权持有者。

18. 如权利要求17所述的卡片式生物辨识方法，其特征在于，该运算处理

模组是透过一无线收发器而以无线传输的方式直接输出该个人资料及该笔待辨
识码至该主机系统。

19. 如权利要求17所述的卡片式生物辨识方法, 其特征在于, 该运算处理
模组是透过一无线收发器而以无线传输的方式间接输出该个人资料及该笔待辨
识码至该主机系统。

20. 如权利要求19所述的卡片式生物辨识方法, 其特征在于, 该间接输出
该个人资料及该笔待辨识别码至该主机系统的方法, 是透过手机或无线网路达成。

21. 如权利要求17所述的卡片式生物辨识方法, 其特征在于, 更包含以下
步骤:

将该笔待辨识别码显示在该卡片式生物辨识装置的一显示器上。

22. 如权利要求17所述的卡片式生物辨识方法, 其特征在于, 更包含以下
步骤:

由该主机系统比对储存于其中的该个人资料是否与该运算处理模组所输
出的该个人资料相符。

卡片式生物辨识装置及方法

技术领域

本发明是关于一种卡片式生物辨识装置及方法，尤其关于一种内含晶片式指纹感测器的生物辨识卡，提供持卡者即时的身份认证，该生物辨识卡可以取代信用卡、个人身份证、驾驶执照、护照、社会福利卡以及医疗健保卡等。

背景技术

信用卡盗刷及假身份证、护照的严重性，使得银行及政府机关每年须花费庞大的人、物力以防止此类的犯罪行为。然而，传统的资料保密方式，例如个人识别号码（Personal Identification Number, PIN）及密码，不仅容易被破解，也会使消费者必须牢记相关的数字。因此，由个人的生物特征作为钥匙便成为一种最经济实惠的方法，特别是指纹特征点的长期稳定性及方便性，使得利用指纹生物辨识卡以取代传统的信用卡、个人身份证、护照以及医疗健保卡等，成为一项重要的技术发展目标。

Lofberg在美国专利第4,582,985号公报中揭露了这一种装置的概念。此种装置的横向尺寸相同于目前通用的信用卡，其主要包含一指纹感测器及一组讯号读取及判别电路。由此对指纹感测器所读取的指纹以及事先储存的指纹资料，即可判断持有者的身份。然而，这种装置仅能提供指示器（譬如LED）来确认持卡者是否为经过授权的持卡者，其意味者只要驱动一张假卡上的指示器也能达到仿冒的目的。

Gullman等人在美国专利第5,280,527号公报中揭露了另一种方法，也就是除了原来的生物辨识外，更增加了一种随时间变化的乱码产生程式，结合确认过的指纹资料，来产生代表个人身份的一组数字，最后再由主机系统根据此数字来解码及/或解密，以产生一组固定码（fixed code）及一修正因子

(correction factor) 来确认身份, 如此可以解决Lofberg发明的缺点。然而, 其所揭露的实施方法必须在主机系统中进行繁复的解密及/或解码动作, 加重了主机系统的负荷, 也会拖慢主机系统的处理速度。同时, 个人身份确认的程序是透过操作员将卡片上所显示的数字记录并输入终端系统, 不仅容易出错, 同时在整个过程中, 辨识装置与终端系统间并无主动式的沟通(interaction), 例如: 如何将个人的资料(I. D. Data)告知终端系统等。

Lane在美国专利第5, 280, 527号公报中揭露了另一种执行方法, 透过磁条作为与主机系统的沟通装置, 有效解决Gullman等人发明的缺点。然而磁条内含的资料是为固定的, 同样的这种方式也会如现有的磁条信用卡一样, 容易被破解。

同时, 在上述的习知技术中, 并无对其所使用的电源作详细的描述。即使上述装置内含有封闭式的电源供应, 但是由于整个指纹比对需要相当大的电源消耗(大于100mA)使得满足此一卡片应用的超薄电池仍然无法支撑产品的长久使用。举例而言, 信用卡或身份证通常为几年换一次而依据上述技术所制造出的信用卡或身份证并无法拥有这么长久的使用寿命。

发明内容

因此, 本发明的一个目的是为提供一种具有高安全性以及长使用寿命的卡片式生物辨识装置, 同时, 兼具标准化、人性化及隐密的沟通界面。

为达成上述目的, 本发明提供一种卡片式生物辨识装置, 用以辨识在一主机系统侧的一待辨识持有者是否为一授权持有者, 该主机系统储存有该授权持有者的一笔个人资料及对应该个人资料的一乱码产生程式。该卡片式生物辨识装置包含一生物感测器、一运算处理模组、一无线收发器及一可充电式电池。生物感测器用以读取并输出该授权持有者的一笔授权生物资料以及该待辨识持有者的一笔待辨识生物资料。运算处理模组用以单次接收、处理并储存该乱码产生程式、该个人资料及该授权生物资料, 然后可多次接收并处理该待辨识生

物资料，并于判断该待辨识生物资料实质上符合该授权生物资料后，透过该乱码产生程式产生并输出一笔待辨识码。无线收发器输出该个人资料至该主机系统，使该主机系统依据对应该个人资料的该乱码产生程式产生一笔授权码，由比较该授权码与该待辨识码，即可判断待辨识持有者是否为该授权持有者。可充电式电池用以提供该运算处理模组、该生物感测器及该无线收发器所需的电源。

本发明亦提供一种生物辨识方法，包含以下步骤：读取并输出一待辨识持有者的一笔待辨识生物资料至一运算处理模组；以该运算处理模组处理并判断该待辨识生物资料是否与一授权生物资料实质上相符；若该待辨识生物资料与该授权生物资料实质上相符，则由该运算处理模组依据储存于其中的一乱码产生程式产生一笔待辨识码；及由该运算处理模组输出一个人资料至该主机系统，使该主机系统依据对应至该个人资料的该乱码产生程式产生一笔授权码，由比较该笔待辨识码及该笔授权码，即可判断该待辨识持有者是否为该授权持有者。

附图说明

图 1 显示依据本发明第一实施例的卡片式生物辨识装置的示意图。

图 2 显示依据本发明第二实施例的卡片式生物辨识装置的示意图。

图 3 显示依据本发明的卡片式生物辨识装置与主机系统的方块图。

符号说明

1	主机系统	2	主控端电脑
3	客户端电脑小卡片式生物辨识装置		
5、5a	生物感测器	6	运算处理模组
7	无线收发器	8	可充电式电池
9	连接器	10	外部电源
11	显示器	12	电源开关
13	生物资料读取开关	14	第一处理器

15	第一记忆体	16	第二处理器
17	第二记忆体	18	第三处理器
19	电源管理单元	20	雷射防伪标签
21	主纹	30	手指

具体实施方式

图1与2显示依据本发明第一及第二实施例的卡片式生物辨识装置的示意图。如图1与2所示，从本发明的卡片式生物辨识装置4的外观可以看出的元件主要包含一生物感测器5或5a、一无线收发器7、一可充电式电池8、一连接器9、一显示器11、一电源开关12及一防伪标签20。此卡片式生物辨识装置4的长度与宽度可以制作成与一般信用卡的尺寸(85mm*5mm)完全相同，而此卡片式生物辨识装置4内部所包含的电子元件及显示器若是采用一般普通的印刷电路板组装方式，则其厚度可以制作成比一般信用卡或智慧卡(smart card)的厚度(约0.8mm)来得厚，大约为2~3mm。而若是为了满足智慧卡的厚度(约0.8mm)要求，则必须将相关的电子元件晶片磨薄(特别是采用一维式的指纹感测器为佳)并且采用COF(Chip On Film)的封装方式方能达到。本发明中采用的可重复充电的高分子锂电池，已可以商品化的厚度小于0.8mm且具有高储电量满足本发明装置的使用，因此在实施上已无大问题。

于此，生物感测器5为一种晶片式指纹感测器(譬如电容式指纹感测器)其可以是一种二维式指纹感测器5(图1)或是一种一维式指纹感测器5a(图2)。于图1中，手指30仅需接触指纹感测器5即可完成指纹的读取，而于图2中，手指30需接触指纹感测器5a并朝着箭头所示的方向滑动。

指纹感测器5或5a是用以读取手指30的指纹21，所读取的指纹21再与预先储存于卡片式生物辨识装置4中的指纹资料比对。由于卡片式生物辨识装置4为一独立辨识装置，故包含了运算能力相当强的微处理器及相关的记忆体(请参见图3)用以对所读取的指纹21进行影像前处理、特征点或特征区块的选取、加密、

解密及比对的动作。或者，该生物感测器5亦可以是声音感测器或数位板。

可充电式电池8可以是一种可重复充电的高分子锂电池，用以供应整个卡片式生物辨识装置4所需的电流。为了达到卡片式生物辨识装置4的运算效能，可充电式电池8的尖峰稳定供电电流须达100至150mA，使处理与比对的动作能在1秒内完成。

此卡片式生物辨识装置4先由个人与卡片的指纹核对确认身份后，再利用内建的可随时间及/或使用次数变化的乱码产生程式来产生一笔代表个人身份的待辨识码（可以是纯数字）上述乱码产生程式譬如揭露于美国专利第4,720,860号公报，其揭露书于此并入作参考。

主机系统中亦储存有该乱码产生程式，用以产生一笔授权码。上述待辨识码可以透过无线收发器7传输至主机系统，由主机系统来核对该待辨识码的正确性。显示器11可以是反射式的液晶显示器，主要用以显示持有者操作过程的资讯以及显示上述待辨识码，以供持有者或操作员作为依据该授权码核对该待辨识码的双重确认正确性。

为了节省电源，本卡片式生物辨识装置4主要由一电源开关12控制电源的供应。为了更进一步识别本卡片式生物辨识装置4的真伪，其外观上更可以包含一防伪标签20，例如全像防伪标签。而本卡片式生物辨识装置4的乱码产生程式可以由各发卡单位或政府单位自行透过微型（譬如RS232或USB连接器等）或平面化的连接器9输入（仅能输入一次）且透过该连接器9也可对可充电式电池8进行充电。

图3显示依据本发明的卡片式生物辨识装置与主机系统的方块图。如图3所示，本发明的卡片式生物辨识装置4是用以辨识在一主机系统1侧的一待辨识持有者是否为一授权持有者。该主机系统1储存有该授权持有者的一笔个人资料及对应该个人资料的一乱码产生程式。卡片式生物辨识装置4包含一生物感测器5、一运算处理模组6、一无线收发器7及一可充电式电池8。为了达成本发明实施例的详细运作功能，卡片式生物辨识装置4可以更包含一连接器9、一显示器11、

一电源开关12及一生物资料读取开关13。该主机系统1包含一主控端电脑2以及与主控端电脑2及卡片式生物辨识装置4连通的一客户端电脑3。运算处理模组6基本上包含一第一处理器14、一第二处理器16、一第三处理器18及一电源管理单元19。第一处理器14通常可包含一第一记忆体15，而第二处理器16通常可包含一第二记忆体17，用以储存资料。

当该发行单位要发行该卡片式生物辨识装置4给该授权持有者时，会将个人资料及专属于个人的乱码产生程式同时输入于该授权持有者的发行单位的主控端电脑2，及该卡片式生物辨识装置4中（是透过连接至该运算处理模组6的连接器9，而将该乱码产生程式及该个人资料传送至运算处理模组6），运算处理模组6仅能单次接收。处理并储存该乱码产生程式及该个人资料，以避免受到盗拷或破解。该乱码产生程式及该个人资料是由第一处理器14接收处理并储存于第一记忆体15中。此外，透过该连接器9亦可接收一外部电源10来对该可充电式电池8充电。

当该授权持有者拿到该卡片式生物辨识装置4时，需要作授权生物资料的输入。举例而言，授权持有者必须在发行单位输入其指纹、声音或签名等生物资料，授权持有者在打开电源开关12后，将卡片式生物辨识装置4置于一磁场产生装置上方以启动本装置内建的生物资料读取开关（譬如磁簧开关reed switch）13，然后对生物感测器5输入授权生物资料。运算处理模组6的第二处理器16接收并处理该授权生物资料，譬如对该授权生物资料进行影像前处理、特征点或区块撷取及加密，再将加密后的资料储存于第二记忆体17中。值得注意的是，将授权生物资料储存至运算处理模组6中的次数仅为一次，且必须在限定的时间内完成，以提高安全性。再者，为了增加辨识的精确度，可以在运算处理模组6中储存有多笔（譬如8笔）的授权生物资料。以目前技术而言，若要在1秒内完成生物资料的辨识动作，则第二处理器16需要具有60MHz以上的运算速度。

当一个待辨识持有者在客户端电脑3有效范围内（意指无线传送接收器的有效范围）使用卡片式生物辨识装置4时，首先打开电源开关12，以使可充电式电

池8对其他电子元件提供电源并同时透过无线收发器7将该个人资料(例如姓名、生日、性别等)告知该客户端电脑3,作为基本身份核对及调取对应该个人资料的该乱码产生程式。若该客户端电脑3完成核对工作,亦回传一适当的讯息(沟通号)至该卡片式生物辨识装置4的无线收发器7,显示于显示器11上,引导待辨识持有者作生物资料输入。反之,若资料核对不符,则此装置无效。接着,待辨识持有者透过生物感测器5输入其待辨识生物资料(譬如指纹、声音、签名等)至运算处理模组6的第二处理器16。第二处理器16处理待辨识生物资料,调出授权生物资料作解密,然后将待辨识生物资料与授权生物资料作比对。当判断该待辨识生物资料实质上符合该授权生物资料后,第二处理器16促使第一处理器14透过第三处理器18及无线收发器7输出生物资料核对成功的资讯于该客户端电脑3,主机系统1与该卡片式生物辨识装置4则透过无线收发器7沟通同步的分别调出对应该个人资料的该乱码产生程式,利用该乱码产生程式产生一笔授权码。同时,该第一处理器14依据该乱码产生程式产生并输出一笔待辨识码与的核对,核对成功的资讯可以显示于显示器11上。而本发明透过无线收发器7与主机系统间作为主动的沟通及同步,可以避免任河人为的操作错误。值得注意的是,该主机系统1亦可以在第一次接收到该卡片式生物辨识装置4所输出的个人资料后,开始调出对应于该个人资料的该乱码产生程式来待命。再者,上述的基本资料核对工作,亦可以视情况而予以调整。而本发明无线收发器7也可以透过间接传送与主机系统1连接,例如透过手机或无线网路连结,这也是本发明装置使用上的弹性及普及特性。

该待辨识码也可以透过第三处理器18而显示在连接至该运算处理模组6的第三处理器18的显示器11上,由操作员目视比对该待辨识码与该授权码作为备用的双重确认,即可判断该待辨识持有者是否为该授权持有者。待辨识生物资料的输入容许多次输入,以允许卡片式生物辨识装置4的长期及多次使用。

本卡片式生物辨识装置4的无线收发器7可以利用符合任河标准传输界面的技术,例如红外线、蓝芽等。运算处理模组6同时内含电源管理单元19,对卡片

式生物辨识装置4内的其他电子元件作电源管理,以期每一次充电至少可以使用70~100次,避免使用上的困扰。值得注意的是,运算处理模组6可以是一种特殊用途积体电路(ASIC)达到微小化的要求。

综上所述,本发明的卡片式生物辨识装置4的生物感测器5是用以读取并输出该授权持有者的一笔授权生物资料以及该待辨识持有者的一笔待辨识生物资料。运算处理模组6是用以单次接收、处理并储存该乱码产生程式、该个人资料及该授权生物资料,然后可多次接收并处理该待辨识生物资料,并于判断该待辨识生物资料实质上符合该授权生物资料后,透过该乱码产生程式产生并输出一笔待辨认证码。无线收发器7是用以输出该个人资料至该主机系统1,使该主机系统1依据对应该个人资料的该乱码产生程式产生一笔授权码。可充电式电池8是用以提供该运算处理模组6、该生物感测器5及该无线收发器7所需的电源。由比较该授权码与该待辨认证码,即可判断待辨识持有者是否为该授权持有者。

此外,运算处理模组6的第一处理器14是用以单次接收、处理与储存该乱码产生程式及该个人资料。第二处理器16是与该第一处理器14及该生物感测器5连通,用以单次接收、处理并储存该授权生物资料,然后可多次接收并处理该待辨识生物资料,并于判断该待辨识生物资料实质上符合该授权生物资料后,促使该第一处理器14输出该笔待辨认证码。第三处理器18是与该第一处理器14连通,用以接收、处理并输出该个人资料及一笔待辨认证码。电源管理单元19是连接至该第一处理器14、该第二处理器16及该第三处理器18,用以作电源管理。

本发明亦提供一种生物辨识方法,用以辨识在一主机系统1侧的持有一卡片式生物辨识装置4的一待辨识持有者是否为该卡片式生物辨识装置的一授权持有者。该主机系统1与该卡片式生物辨识装置都储存有该授权持有者的一笔个人资料及对应该个人资料的一乱码产生程式,而该卡片式生物辨识装置4储存有该授权持有者的一笔授权生物资料。

执行本发明的方法时,首先读取并输出该待辨识持有者的一笔待辨识生物资料至一运算处理模组6。然后,以该运算处理模组6处理并判断该待辨识生物

资料是否与该授权生物资料实质上相符。若该待辨识生物资料与该授权生物资料实质上相符,则由该运算处理模组6依据储存于其中的该乱码产生程式产生一笔待辨识码。接着,由该运算处理模组6输出该个人资料至该主机系统1,使该主机系统1依据对应至该个人资料的该乱码产生程式产生一笔授权码。由比较该笔待辨识码及该笔授权码,即可判断该待辨识持有者是否为该授权持有者。将该笔待辨识码可以显示在该卡片式生物辨识装置4的一显示器11上,或者可以被传输至该主机系统1。

简言之,本装置除了由连接器作一次乱码产生程式与个人资料的输入及重复性充电外,主要是透过无线传输送出个人资料(无线传输亦包含了加密功能)且不须与任何终端系统接触,彻底避免任何盗拷或破解的机会,提供了最安全性的设计,而且标准的无线传输界面,提高了与主机系统沟通的便利性及隐密性,也避免了人为犯错的机会,可重复充电的设计,更使本装置可以长期使用,解决了使用便利性及流通性的问题。由于乱码产生程式不需要运算速度相当高的处理器即可运作,故本发明在主机系统1亦不会造成相当的负载。

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。

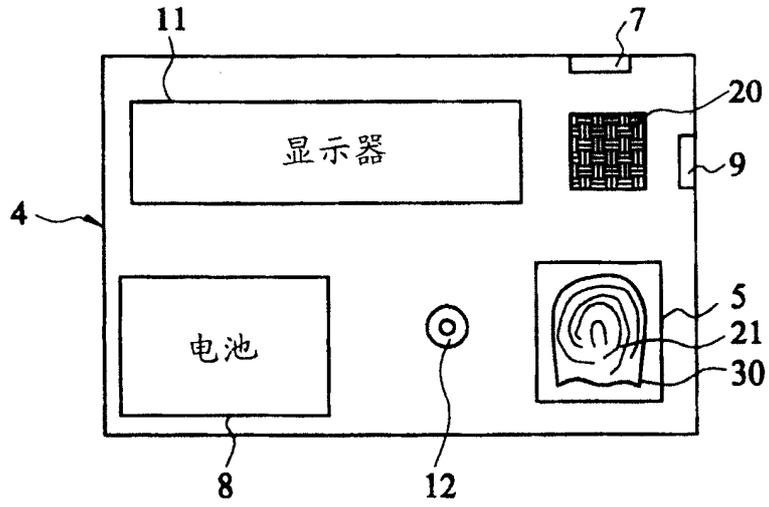


图1

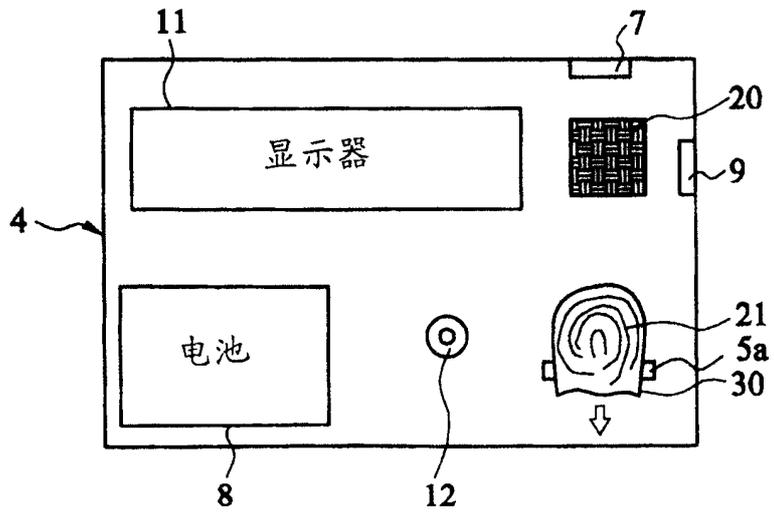


图2

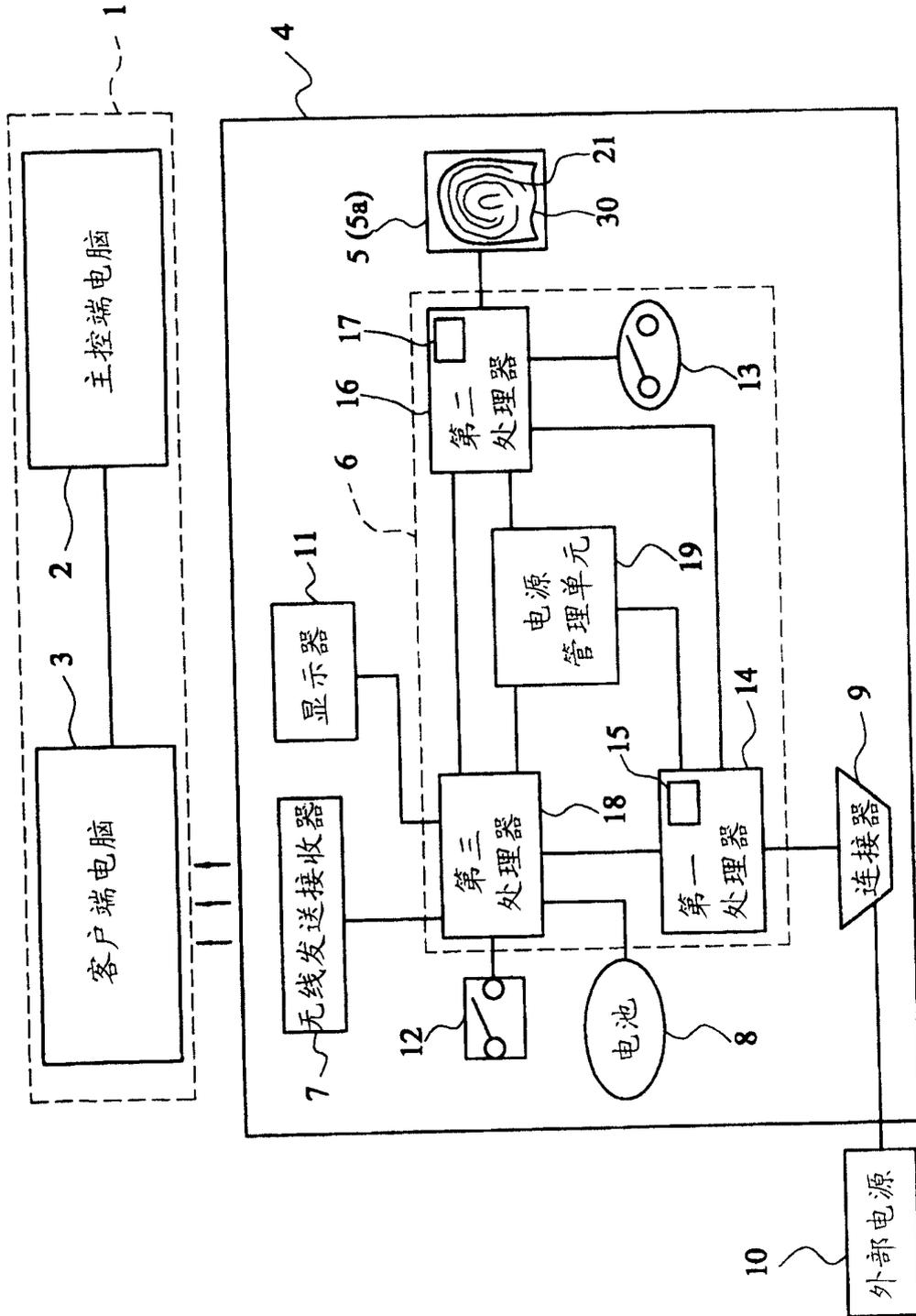


图3