[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
G06K 19/077
C07C 9/00

[12] 发明专利申请公开说明书

[21] 申请号 03825009.8

[43] 公开日 2005 年 11 月 9 日

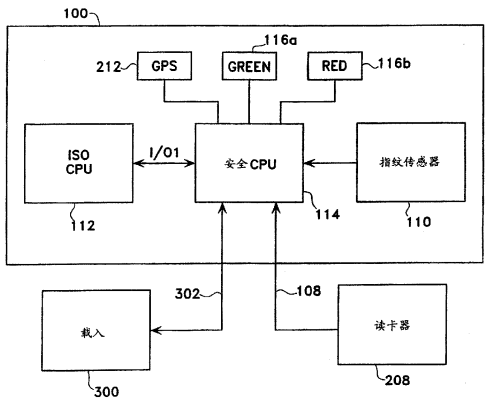
[11] 公开号 CN 1695163A

[22] 申请日 2003.9.10 [21] 申请号 03825009.8
[30] 优先权
[32] 2002. 9.10 [33] US [31] 60/409,716
[32] 2002. 9.10 [33] US [31] 60/409,715
[32] 2002.11.27 [33] US [31] 60/429,919
[32] 2002.12.13 [33] US [31] 60/433,254
[32] 2003. 7. 3 [33] US [31] 60/484,692
[86] 国际申请 PCT/US2003/028602 2003.9.10
[87] 国际公布 WO2004/025545 英 2004.3.25
[85] 进入国家阶段日期 2005.5.9
[71] 申请人 艾维智能技术有限公司
地址 美国加利福尼亚州
[72] 发明人 塔米奥·萨伊托 会田 刚
韦恩·德里辛
[74] 专利代理机构 北京康信知识产权代理有限责任公司
代理人 余 刚
权利要求书 4 页 说明书 29 页 附图 10 页

[54] 发明名称 安全的生物身份验证

[57] 摘要

本发明公开了一种高安全性身份识别卡，包括用于存储生物数据的卡上存储器，用于获取现场生物数据的卡上传感器。 卡上的卡上处理器执行匹配操作，以验证获取的生物数据与本地保存的生物数据的匹配。 仅当存在正确的匹配时，其它数据才可以从卡中传出以做附加验证和/或进一步处理。 优选地，卡与 ISO 智能卡(ISO SmartCard)兼容。 在一个实施例中，ISO 智能卡起防火墙的作用，用于保护用来保存和处理受保护生物数据的安全处理器免遭通过 ISO 智能卡接口进行的外部恶意攻击。 在另一实施例中，安全处理器插于 ISO 智能卡接口和无变更 ISO 智能卡处理器之间并一直阻止任何外部通讯直到用户的指纹已经与先前注册的指纹相匹配为止。 当用户将其手指放到指纹传感器上方时，实时反馈被提供，从而有助于手指在传感器上方进行最佳放置。 卡可以用来启动与交易网络的通讯或获得进入安全区域的物理通道。



ISSN1008-4274

1. 一种智能身份识别卡，包括：

卡上存储器，用于储存参考数据；

卡上传感器，用于捕获现场生物数据；

卡上微处理器，用于在预定阈值内将所捕获的生物数据和相应的存储的参考数据进行比较，且仅当在预定阈值内匹配时才产生验证消息，以及

用于将所述验证消息发送到外部网络的装置。

2. 根据权利要求 1 所述的身份识别卡，其中，所述验证消息至少包括来自所存储的参考数据的摘录。

3. 根据权利要求 2 所述的身份识别卡，其中，所述验证消息至少包括来自所捕获的生物数据的摘录。

4. 根据权利要求 3 所述的身份识别卡，其中，所述验证消息被传输到远程认证系统用于附加的验证。

5. 根据权利要求 4 所述的身份识别卡，其中，所述远程认证系统包括与所述本地存储的参考数据不同的远程存储的参考数据。

6. 根据权利要求 4 所述的身份识别卡，其中，所述卡上微处理器使用与所述远程认证系统不同的匹配算法。

7. 根据权利要求 2 所述的身份识别卡，其中，所述整个匹配程序由所述卡上处理器执行并且不将所捕获的生物数据发送到所述网络。

8. 根据权利要求 2 所述的身份识别卡，其中，存储在所述卡上存储器里的原始捕获的生物数据以及任何其它“私有”信息对于任何外部程序都是不可用的。

9. 根据权利要求 2 所述的身份识别卡，其中，所述卡是 ISO 兼容智能卡。

10. 根据权利要求 9 所述的身份识别卡，还包括 ISO 智能卡处理器。

11. 根据权利要求 10 所述的身份识别卡，其中，用于储存和处理所述受保护的生物数据的所述安全处理器被防火墙从功能上与所述 ISO 智能卡处理器隔离。

12. 根据权利要求 10 所述的身份识别卡，其中，进出所述安全处理器的所有外部数据均通过所述 ISO 智能卡处理器。

13. 根据权利要求 10 所述的身份识别卡，其中，进出所述 ISO 智能卡处理器的所有外部数据均通过所述安全处理器。

14. 根据权利要求 10 所述的身份识别卡，其中，所述安全处理器具有：第一连接，用于在载入程序期间载入数据；以及第二连接，连接到外部网络。

15. 根据权利要求 14 所述的身份识别卡，其中，使所述第一连接在所述载入程序完成之后永久禁用。

16. 根据权利要求 10 所述的身份识别卡，其中，用于存储和处理所述受保护的生物数据的所述安全处理器被防火墙从功能上与所述 ISO 智能卡处理器隔离。

17. 根据权利要求 10 所述的身份识别卡，其中：

所述卡包括上磁条区域和下浮雕区域；

所述生物传感器是指纹传感器；以及

所述安全处理器、所述 ISO 智能卡处理器和所述指纹传感器均位于在所述上磁条区域和所述下浮雕区域之间的中间区域。

18. 根据权利要求 2 所述的身份识别卡，其中，所述生物数据包括指纹数据并且所述传感器是用于从放在所述传感器上的用户的手指获取数据的指纹传感器。

19. 根据权利要求 18 所述的身份识别卡，其中，当所述用户将其手指放到所述指纹传感器上方时，提供实时反馈，从而有助于所述手指在所述传感器上方进行最佳放置。

20. 根据权利要求 18 所述的身份识别卡，其中，所述匹配程序采用混合匹配算法，所述混合匹配算法考虑了所捕获的生物数据中的细节和全部空间关系。

21. 根据权利要求 18 所述的身份识别卡，其中，所述指纹传感器包括通过垫板支承的晶体硅片。

22. 根据权利要求 21 所述的身份识别卡，其中，所述垫板包括夹在两个金属层之间的玻璃环氧树脂层。

23. 根据权利要求 18 所述的身份识别卡，其中，所述垫板由围绕所述硅片的载体框加固。

24. 根据权利要求 1 所述的身份识别卡，其中，所述卡还包括用于将所述卡的使用限定于预定位置的装置。

25. 根据权利要求 1 所述的身份识别卡，其中，所捕获的生物数据中的至少一部分和所述参考数据被传输到独立的认证服务器，用于在任何授权在线访问用于处理涉及此用户的安全金融交易的应用服务器之前对用户身份进行安全验证。

26. 根据权利要求 25 所述的身份识别卡，其中，响应于涉及在所述认证服务器上产生肯定匹配的特定应用服务器上的特定登录企图的匹配请求，执行安全三路认证协议，其中将询问字符序列从所述认证服务器发送到所述身份识别卡，然后所述身份识别卡使用所述询问字符序列和所述匹配请求产生询问响应，然后将其发送到所述应用服务器，然后所述应用服务器将所述询问响应发送到所述认证服务器，然后所述认证服务器确认所述询问响应是否有效。

27. 根据权利要求 1 所述的身份识别卡，其中，所述卡的所述输出用于获得进入安全区域的物理通道。

28. 根据权利要求 27 所述的身份识别卡，其中，成功和不成功访问企图的记录都被保存在所述卡中。

安全的生物身份验证

相关申请

本发明基于如下临时申请，2002 年 9 月 10 日提交的第 60/409,716 号（卷号为 7167－102P1）、2002 年 9 月 10 日提交的第 60/409,715 号（卷号为 7167－103P）、2002 年 11 月 27 日提交的第 60/429,919 号（卷号为 7167－104P）、2002 年 12 月 13 日提交的第 60/433,254 号（卷号为 7167－105P）、2003 年 7 月 3 日提交的第 60/484,692 号（卷号为 7167－106P），并且要求这些申请的优先权，这些申请的全部内容结合于此作为参考。

技术领域

计算机化特别是互联网技术已经提供了对包括财务数据、医疗数据、个人数据的不断增长的数据访问，这意味着加速了金融和其它交易，其中保密数据被进行更新或者交换。

通常用口令来维持这些数据的保密性；然而，口令经常是基于易于猜测并且根本就不安全的出生日期或者电话号码。此外，即使是复杂的随机生成的口令也经常能被轻易窃取。基于口令的数据访问系统因而容易受到非法攻击，从而给工业和经济，甚至给人的生命带来危险和损害。因此，需要一种改良的方法，用于保护数据和保护数据免遭未授权访问。

生物数据可以包括难以获取但是容易分析的精密细节（例如指纹细节序列），或者容易获取但是难以分析的整体图案（例如相邻指纹螺纹的空间特性）。

加密算法需要仅对授权用户有效的数字密钥。没有正确的密钥，只有投入足够的时间和处理资源，而且即便如此，只有当未加密数据的某些特征是已知的（或者至少是可预知的）时，加密数据才可以被解密成可用格式。

日本公开专利申请第 60-029868 号（日期 1985 年 2 月 15 日，申请人为 Tamio SAITO），提出一种个人识别系统，其使用一种具有用于记录从持卡人处获得的加密生物数据的集成存储器的身份识别卡。生物数据可以包括声波纹、指纹、外貌特征、和/或生物检验。使用中，卡中数据被读取和解密，用于与从出示该卡的人处获取的相应数据进行比较。该系统使得注册人可被高准确度地确定识别。然而，因为生物数据是通过外部设备获得和处理的，所以难以保护存储在卡上的信息免遭可能发生的改变和/或身份盗用。

已经提出了一种改良的身份识别卡，其包括卡上的数据驱动多处理器芯片，以提供同时加密和隔离存储在卡上的生物数据的硬件防火墙，从而提供更好的保护来防止未经授权而改变存储数据。然而，实际的匹配程序是在同样的获取现场（live）生物数据的外部读卡器终端上执行的，因而仍然潜在地容易受到外部欺诈操作的攻击。

发明内容

高安全性身份识别卡的第一实施例不仅包括用于存储生物数据的卡上（on-board，又称片上或板上）存储器，而且包括用于捕获现场生物数据的卡上传感器。远程认证系统维护包括生物数据的

安全数据库。卡上的卡上处理器执行初步的匹配操作，以验证所捕获的生物数据与本地生物存储数据是否匹配。仅当存在正确的本地匹配时，任何获取的数据或任何敏感的存储数据才可以发送到远程认证系统用于附加的验证和/或进一步处理。作为对于恶意攻击的进一步保护，本地存储数据优选不同于远程存储数据，并且优选地使本地匹配和远程匹配采用不同的匹配算法。因而即使卡、本地存储数据、和/或与卡连接的本地终端遭受损害，很可能地，远程认证系统仍然能够发觉入侵企图。

第二实施例也包括用于存储生物数据的卡上存储器、用于捕获现场生物数据的卡上传感器、以及卡上处理器；然而，在该实施例中，整个匹配程序由卡上处理器来执行，并且生物原始获取数据和存储在卡上存储器中的任何其它“私有”信息对于任何外部程序都是不可访问的。替代地，响应于在新获取的生物数据和先前获取的生物数据之间的成功匹配，仅产生一个验证信息。验证信息使得该卡功能类似于依据了传统的个人身份号码（PIN）的登录（log on）成功/不成功的传统ISO智能卡的方式，但是其具有由更多的安全验证程序所提供的附加的安全性。在任一实施例中，生物存储数据和任何相关的本地存储的加密算法或者加密密钥优选地在最初授予持卡人时载入卡中，其方式为阻止任何将来的外部访问，从而进一步增强了生物存储数据和整个验证程序的完整性。

在一个实施例中，ISO智能卡起到防火墙的作用，用于保护用来存储和处理受保护生物数据的安全处理器免于遭受通过ISO智能卡接口进行的外部恶意攻击。在另一个实施例中，安全处理器插于ISO智能卡接口和没有经过修改的ISO智能卡处理器之间，并一直阻止任何外部通信直到用户的指纹已经与先前注册的指纹相匹配为止。

在具有卡上指纹匹配能力的高安全性身份识别卡的一个优选实施例中，当用户将其手指放到指纹传感器上方时，实时反馈被提供，从而有助于手指在传感器上方进行最佳放置。该反馈不仅降低了计算复杂性，而且提供了用于在无经验用户和欺诈用户之间进行区别的附加方法，从而进一步减少了错误否定和/或错误肯定的可能性。在另一个优选实施例中，指纹传感器被保持在提供额外稳定性的载体中。

在一个示范性应用中，将获取到的生物数据和/或持卡人的身份标志在任何对保密数据在线访问的授权之前或者在任何用于完成安全交易的自动化程序之前进行加密，然后输入到包括金融机构和单独的认证服务器的交易网络中。在另一个示范性应用中，将卡的输出用于获得进入安全区域的物理通道。在任一应用中，成功的和不成功的访问企图的记录都可以被保存在卡上或者外部安全服务器上，或者在两者上都保存。

附图说明

图1示出了具有卡上生物验证示卡人的身份的智能卡的一个实施例；

图2是用于帮助用户实现手指在指纹传感器上的最佳放置的示范性程序的流程图；

图3是能够同时本地和远程验证出示安全身份识别卡的人的身份的生物验证系统的功能方框图；

图4是具有在初始载入持卡人生物数据期间和在验证持卡人的远程请求身份期间使用不同物理数据路径的典型的生物验证卡的功能方框图；

图 5 示出了图 4 的典型生物验证卡的可选实施例，其打算采用无修改的 ISO 智能卡 CPU 的方式；

图 6 是表示典型应用和典型验证卡之间的通信的流程图，其中只执行对持卡人身份的本地验证；

图 7 是类似于图 6 的流程图，但是改为采用图 5 的典型生物验证卡的方式；

图 8 示出了具有可无线或者借助于电接插件连接到本地终端的卡上生物验证的智能卡的第二实施例；

图 9 是图 8 的卡的横截面图；

图 10 是典型指纹传感器的电路图；以及

图 11 示出了用于图 10 的传感器的载体组件的一个实施例。

具体实施方式

智能卡

此处使用的术语“智能卡（smart card）”或者“智慧卡（intelligent card）”一般意义上是指任何物理对象，其足够小到可以握在手中，戴在脖子上，或者以其它方式随身携带，其包括微处理器，能够存储、处理和传递涉及或者其它关系到持卡者个人的数字编码信息。这种智能卡的一个众所周知的实例是 ISO（International Standards Organization 国际标准组织）智能卡，其具有与传统的信用卡相同的物理尺寸和外形，但是其包括：闪存，用于存储用户特定数据；以及微处理器，能以强大的加密算法进行编程，指示从用户终端收到的 PIN（Personal Identification Number 个人身份号码）是否与卡

上存储的加密 PIN 相匹配，从而与仅依靠对签名和/或身体相貌进行视觉比较的验证系统相比，对出示卡的人是真正的持卡人给出了更高的可信度。

接下来参照图 1，其示出了具有卡上生物验证的智能卡的一个实施例。卡 **100** 通常由塑料材料制成，并且具有传统的信用卡的整体外观，其大致尺寸符合 ISO7816 中规定的约 53.98 × 85.6mm 且厚度约 0.76mm 或者更厚。

类似于传统的信用卡，卡 **100** 包括空白的上部区域 **102**，其沿着卡的整个横向宽度延伸，用于承载位于卡的背面上的磁条（符合 ISO7811-2&7811-6 的规定），该磁条上可以存储关于持卡人和任何相关帐户的传统编码字符信息，从而使卡 **100** 可在传统的磁条读取器中使用。然而，因为载入磁条中的任何数据都易于修改，所以这样的磁条仅仅适用于对老式磁条式终端的向后兼容的需要超过磁条带给系统安全性的潜在下降的特定应用中。

上部区域 **102** 还用于支持各种防伪措施，例如持卡人的防篡改的彩色照片和/或发卡人的全息标识。卡 **100** 的下部区域 **104** 可以使用传统样式的浮雕信息（符合 ISO 7811-1 规定），例如持卡人姓名、数字帐（或者卡）号、以及有效日期，以使卡 **100** 可在传统的卡刻印器中使用。

上部区域 **102** 和下部区域 **104** 被中部区域 **106** 分隔，其中嵌入一组 8 个可见的 ISO 智能卡触点 **108**，其在卡和读卡器上相应触点之间提供方便的电连接。通过该方法，不仅数据，而且电源、时钟以及控制信号都可在读卡器和卡之间进行交换，如 ISO 7816-3 中所规定的。

在区域 **106** 的右侧可以看见传感器区域 **110**，其用于从持卡人的手指获取指纹数据。优选地，向卡提供与传感器 **110** 或者嵌入卡中其它电子元件唯一对应的 ID 码；例如，传统的 IP 和/或 MAC 地址格式的编码。

图 1 还示意性地示出了数个附加的电子元件，其与触点 **108** 和传感器 **110** 配合，与其他可能相比，提供了更强大的功能，特别是更好的安全性。

在一个实施例中，ISO 智能卡兼容处理器 **112** 直接连接到 ISO 触点 **108**，以提供与外部 ISO 兼容读卡器（未示出）的电连接，从而不仅向卡上电子器件提供电源，而且提供用于在卡与任何运行在读卡器或者任何与读卡器联网的相关计算设备上的外部通信软件、安全软件、交易软件、和/或其它的应用软件之间传输数据的方法。

尽管在所述实施例中，在卡 **100** 和外部读卡器之间的数据通道是使用 ISO 规定的智能卡连通方案的有线连接的形式，但应当明白，在其它的实施例中，其它的传输技术也可以被使用，例如 USB 或 RS 232C 或 SPI（串行）连接，可通过无线 RF（Radio Frequency 射频）、微波和/或 IR（InfraRed 红外线）通信链路。

同样，尽管所述实施例从读卡器获取电源，但其它的实施例可以具有卡上电源，例如太阳能电池或者电池。该卡上电源可能具有优势，例如，如果在卡 **100** 和特定类型读卡器之间的机械接口是这样的，以使指纹传感器 **110** 在触点 **108** 连接到读卡器中相应连接的情况下不能被用户访问，从而必须在卡 **100** 不与读卡器直接有线连接的情况下捕获用户指纹数据。

安全处理器

如图所示，安全处理器**114**连接在ISO处理器**112**和传感器**110**之间，用于提供对所捕获的数据的安全处理和存储，并且提供“防火墙”，以保护存储在它的专用存储器中的数据和程序免遭任何通过ISO处理器**112**进行的异常访问企图，如下文所述。该防火墙可设计为仅通行使用了加密密钥的加密数据，该加密密钥基于唯一分配的网络地址或者其它与该特定卡唯一对应的东西，例如从先前存储的指纹图案提取的数据，或者唯一分配的设备号例如 CPU 号，或者指纹传感器号。在另一个实施例中，防火墙仅仅通行包括源自先前的传输或者数据的唯一可识别数据的数据。在其他实施例中，防火墙对不同的应用保存不同的密钥，并且用这些密钥将数据发送到各自不同的处理器或者存储器部分。

在另一个实施例中（未示出），安全处理器**114**直接连接到ISO触点**108**，并且充当ISO处理器**112**与ISO触点**108**之间的安全门禁。该可选方案具有如下优点，提供由安全处理器**114**和传感器**110**提供的附加的安全性，而不会有任何危及任何可能已集成到ISO处理器**112**中的安全特性的可能。

安全处理器**114**优选包括非易失半导体存储器或者非半导体存储器，例如FRAM、OTP、E^2PROM、MRAM、MROM，用于存储先前注册的指纹图案和/或其它的人体生物信息。在其他实施例中，安全处理器**114**的一部分或者全部功能可在ISO处理器**112**中执行，和/或ISO处理器**112**的一些或者全部功能可在安全处理器**114**中执行。这样的组合执行仍能维持各功能之间的软件防火墙，如果设备以不允许对存储的软件程序作任何后续修改的方式来执行，那么这将是特别有利的。可选地，处理器**112**、**114**都可以是单个多处理器设备中单独的处理器，该设备设计为保护每个处理器免遭来自运行

在不同处理器内的另一个程序的任何干扰。这种多处理器装置的一个实例是日本夏普公司（Sharp）的 DDMP（Data Driven Multiple Processor，数据驱动式多处理器）。

尽管这些各种传感器、触点、和其它电子元件，以及用于互连的印刷电路或者其它电线路，均优选被完全装入卡 **100** 的卡体，从而保护它们免遭磨损和外部污染，而且还在上部区域 **102** 和下部区域 **104** 之间的中间区域 **106** 之内的优选位置进一步保护它们免遭来自与其它区域有机械连接的传统的磁条读卡器、压印机、以及刻印装置的可能的损害。

LED 反馈

LED **116a**、**116b** 由安全处理器 **114** 控制，向用户提供可视反馈。在所示实施例中，它们位于下部区域 **104** 中，优选地位于卡的侧边远离触点 **108** 的位置。无论如何，LED **116a**、**116b** 优选地位于在任何压印程序期间它们不会被损害的位置，以及位于当卡插入传统的 ISO 智能卡读取器时和/或当用户手指放到指纹传感器 **110** 上方时它们可以被看见的位置。例如：

在验证模式下：

- 红灯闪烁：等待手指
- 停止闪烁：手指已放在传感器上
- 红灯闪烁一次：不匹配，可以移动手指
- 绿灯长闪烁一次：已匹配，可以移开手指

注册模式下：

- 绿灯闪烁：等待手指
- 停止闪烁：手指已放在传感器上

- 红灯闪烁一次：不能注册，可以移动手指
- 绿灯闪烁一次：已注册，可以移开手指

擦除模式下：

- 绿灯和红灯闪烁：准备擦除
- 绿灯闪烁一次：已擦除

优选地，在发送任何否定报告之前，用户被给予多次机会去放置其手指以得到成功的匹配或者注册。在一个实施例中，只有当用户在收到绿灯准许指示之前移开其手指时，或者当预定时限超出时，否定报告才被发送到认证服务器。该程序不仅训练用户实现其手指在传感器上方进行最佳放置，其不仅降低了计算复杂性，而且使得可使用更大的辨别阈值。该可视反馈还提供了用于在无经验用户（其通常不断尝试直到实现正确的放置）和欺诈用户（其通常不希望引起任何注意，并且将会在其恶意被发觉之前离开）之间进行辨别的心理学基础。最终结果是显著减少了错误否定和/或错误肯定的可能性。

图 2 示出了帮助用户将其手指放置到传感器 **110** 上的典型程序。在方框 **150** 中，RED LED **116b** 正在闪烁。一旦手指被探测到（方框 **152**），该 LED 就停止闪烁并进行图像质量（对应于手指皮肤的凸部和凹部的细长的限定区域）的检测（方框 **154**）。如果质量不合格（NO 分支 **156**），那么 RED LED **116b** 的单次闪烁指示用户移动其手指到不同的位置（方框 **158**）；否则（YES 分支 **160**）执行第二检测（方框 **162**），以确定是否相同手指放在被用来注册用户的相同位置，从而相对简单的匹配算法就可在预定阈值范围内验证现场数据与存储数据的符合，从而验证现场手指与最初注册的手指相同（YES 分支 **164**），以及 GREEN LED **116a** 被激活（方框 **166**）持续足够长时间（方框 **168**）以证实已经产生成功的匹配以及用户现

在可以移开其手指。可选地，如果匹配阈不满足（NO 分支 **170**），那么红色 LED **116b** 的单次闪烁（方框 **158**）指示用户移动其手指到不同的位置，且该程序重复进行。

典型网络结构

接下来参照图 3，其示出了既可本地也可远程验证出示安全身份识别卡的人的身份的生物验证系统的一个可能的实施例。其包括三个主要部分:客户终端 **200**,应用服务器 **202** 以及认证服务器 **204**。客户终端 **200** 包括以下功能：现场捕获和本地处理用户的指纹、加密本地处理数据、以及与应用服务器及认证服务器进行安全通信，该安全通信优选通过使用 IP/TCP 寻址方案和传输协议的互联网进行，并通过传统的 IP 防火墙 **206** 提供保护以免遭恶意访问。在其他实施例中，防火墙 **206** 可以拥有过滤器以及加密编码器/解码器，用于当发送数据被验证为授权数据后将其编码并用于当确定接收数据是否为授权数据前将其解码，其例如使用像 DES **128** 这样的加密算法。用该方法，防火墙 **206** 不仅可根据报文头，而且可根据报文内容来将数据分类为授权数据或者潜在恶意数据。

客户终端 **200** 可以专用网络设备的方式来实现，或者可以应用于安装在可编程的台式电脑、笔记本电脑或者其它工作站或个人电脑上的软件当中，这些电脑由通用操作系统例如 Windows XXX、OS X、Solaris XX、Linux 或 Free BSD 所控制。优选地，客户终端 **200** 包括保持更新的“禁用”数据库（例如丢失的或者失窃的卡的身份，或者对特定的卡或者一组卡的限制），以提供附加的安全措施。

应用服务器 **202** 包括如下功能，进行事务处理，或者在用户的身份已经被认证服务器 **204** 证实之后，响应来自在客户终端 **200** 的远程用户的指令。认证服务器 **204** 包括以下功能，与客户终端 **200**

及应用服务器 **202** 进行安全通信，存储真实指纹数据和其它关于前注册用户的信息，将存储数据与从客户终端 **200** 收到的加密的现场数据进行比较，以及通知应用服务器 **202** 指定的现场指纹数据是否匹配存储的指纹数据。

更特别地，客户终端 **200** 还包括两个主要部件：固定读卡器 **208** 部件，其包括互联网浏览器终端 **210** 和读卡器接口 **108a**（其可以是简单的 USB 线缆，端接在一组电触点上，用于形成与 ISO 智能卡触点 **108** 的对应电连接）；以及便携式智能卡部件 **100'**。在一个实施例中，便携式部件 **100'**可以是前面所述的智能卡 **100**，包括指纹传感器 **110**、安全处理器 **114** 和 ISO 智能卡处理器 **112**。

应用服务器 **202** 还包括互联网服务器接口，其包括防火墙 **206** 和互联网浏览器 **214**，以及交易应用模块 **216** 和确认模块 **218**。在应用服务器和应用模块 **216** 是未被设计成通过 IP/TCP 协议进行对外通信的传统设备的情况下，防火墙 **206** 可用适当的安装了确认模块 **218** 并且具有固定 IP 地址的协议转换程序来代替。例如，应用服务器可以由愿意通过互联网向授权用户提供服务的第三方来进行操作。

认证服务器 **204** 还包括：互联网服务器接口 **220**；处理模块 **222**，包括指纹匹配算法 **224**；以及数据库 **226**，用于存储指纹和其它当这些个人被系统注册以及其身份保证满足系统操作员的要求时从这些个人处收集的真实信息。为了进一步加强安全性，优选地，用于任何特定个人的存储数据不以单一的信息列来存储在应用服务器上，而是将各项分开存储，并且任何连接这些项目所要求的索引或者关联都只有通过相应的密钥才可以得到，该密钥保存为认证服务器中个人私人数据的一部分。

定位

在某些实施例中，固定读卡器 **208** 和/或便携式卡 **100"**还可以装备集成的全球定位卫星（Global Positioning Satellite，“GPS”）接收器 **212**，其可提供关于读卡器和卡在或约在特定交易发生时的当前位置的有用信息。特别地，来自 GPS 接收器 **212** 的位置数据可用于在读卡器或卡被移出至其使用未获授权的区域的情况下使读卡器和/或卡失效（永久或临时）。除了通过 GPS，还可以通过其他方法来自动确定位置，例如采用 PHS（日本蜂窝式电话）呼叫者定位技术，或者采用对地球电磁场中的局部变化敏感的定位传感器。在装备 GPS 卡的特别例子中，各种 GPS 元件包括天线；数字放大、AD 转换器以及采样和保持电路；以及计算位置的数字信息处理器，优选地，这些元件都是单块集成电路的部件或者都是安装在单块电路板上的分立器件，其被集成、嵌入或者层压到卡体中。

具有卡上匹配的 ISO 卡的卡结构

ISO 处理器接口

图 4 是典型 ISO 智能卡兼容生物验证卡 **100** 或 **100'**的功能方框图，其有不同的物理数据路径，用于初始载入持卡人生物数据期间和验证持卡人对远程应用的身份期间。

特别地，除了前面描述的 ISO 处理器 **112**、安全处理器 **114**、指纹传感器 **110**、LED **116a**、**116b** 和可选的 GPS 接收器 **212**，其中只有 ISO 处理器 **112** 通过 ISO 智能卡触点 **108** 直接连接到读卡器 **208** 的方式之外，还示出了独立的加载模块 **300** 和相关的临时连接 **302**，其在初始的用户注册期间提供与安全处理器 **114** 的直接通信。可以注意到，当临时加载连接 **302** 连接到特定的 I/O 端口 **308** 时，ISO 处理器 **112** 通过 I/O 端口 **304**、**306** 与安全处理器 **114** 进行通信。

优选地，安全处理器编程为，使得任何敏感保密相关数据或者软件仅可从端口 **308** 得到而不能从端口 **304** 和 **306** 得到，从而避免了在连接 **302** 被禁止后任何恶意访问这些敏感数据的可能性。

大多数市场上可获得的ISO处理器具有至少两个I/O端口而且有些具有至少三个。这些端口中仅有一个（I/O 1）被指定用于连接到外部ISO兼容读卡器 **208** 的传统的ISO智能卡串行数据连接 **108**。优选地，另外的一个或者两个I/O端口提供了在ISO处理器 **112** 和安全处理器 **114** 之间的专用硬布线通信，其作为硬件防火墙，以阻止对安全处理器 **114** 重编程序或者获得对任何敏感信息的访问的任何恶意企图，该信息可能是先前被传感器 **110** 获取或者可能是被存储在处理器 **114** 内。在具有多于两条I/O线路的ISO处理器的特定情况中，甚至当安全处理器完全断电时，可能在ISO处理器和安全处理器之间的专用通信路径上的静态信息出现多于两个的状态，例如1）Ready（就绪），2）Busy（忙），3）Fail（失败），和4）Pass（通过）。当然，即使只有一个I/O端口有效，这四种状态也能作为串行数据被动态发送。

可以通过ISO接口I/O 2和I/O 3在ISO CPU与安全CPU之间传输的可能的命令和数据如下：

- 注册或者验证用户命令，安全CPU将对其发送注册结果或者验证结果，用于本地存储和/或发送至远程应用。
- 指纹信息，作为模板（参考）可从安全CPU发送到ISO CPU，用于存储到ISO智能卡存储器中以发送至远程应用。为了加强敏感私人信息的安全性，参考数据可在其发送到ISO CPU之前由安全CPU进行加密。

加载连接 **302** 提供与安全CPU **114** 的直接连接，当可在ISO CPU **112** 和ISO读卡器 **208** 之间维持通信时，其绕开ISO连接和相

关的专用 I/O 端口 **304** 和 **306** 所提供的任何防火墙保护，从而电源对于安全 CPU **114** 也是可用的。主要是用于该卡对特定用户的初始注册，并将可防止未授权访问。

图 5 示出了图 4 所示的典型生物验证卡的可选实施例，其打算使用未修改 ISO 智能卡 CPU（unmodified ISO SmartCard CPU）。特别地，ISO CPU **112'**无论在正常使用期间或者在装载期间都不必再在读卡器 **208** 和安全 CPU **114'**之间执行任何网关功能，因而其可以是任何 ISO 许可芯片，其不以任何方式作改变，并且以对读卡器 **208** 和对任何外部应用都绝对透明的方式来使用。在该可选实施例中，如果获取的指纹和存储的指纹相匹配，那么安全 CPU **114'**就用作 ISO CPU **112'**和任何外部应用之间的透明防火墙，并且如果获取到的指纹和存储的指纹不匹配，那么其将阻止所有这些通信。

卡初始化和存储数据的保护

剪断

在一个实施例中，最初制造的卡具有突出的印刷电路延伸物，其提供与安全 CPU，以及与至少 ISO 接口的部分和/或任何分立的卡上存储器的直接连接。直接连接接口仅仅用于检测卡和指纹注册数据，并且包括使注册程序生效的信号。注册完成后，将电路延伸物机械地断开，从而不再可能进行注册，并且安全 CPU 存储器只有通过 ISO CPU 和前面描述的 ISO CPU 与安全 CPU 之间的防火墙才可进行访问。

保险丝

在另一个实施例中，安全 CPU 有一种存储器，一旦将注册指纹图案写入，其就将不可访问。该存储器的一个实例是一次性 PROM（“OTP”），其在结构上和 EEPROM 相似，但是对 UV 不透

明，因而不可擦除。另一个实例是 Flash ROM，其在注册完成之后变成只读，例如对 Enable 或 Address 或 Data 信号路径通过施加足够的电流，以在该信号通道中形成物理断路（“保险丝”）。

典型认证程序

在一个实施例中，典型认证程序包括获取物理指纹数据，例如，在由访问人使用的连接到应用服务器的客户终端上使用光学或压力或传导或电容或声学或弹性或摄影技术，然后将该数据发送（优选地，以加密格式）到独立的指纹认证服务器。指纹认证服务器使用认证软件将获取的指纹数据与指纹文件进行比较，该文件包括用户的指纹注册数据，并且如果数据是匹配的，那么认证服务器发送生效指令到应用服务器。

在另一个实施例中，用户访问指纹认证服务器的安全网络浏览器，其包括指纹文件，其中所有指纹连同个人数据一起是预注册的，例如姓名、地址、和出生日期。然后用户通过安全协议例如 HTTPS 格式访问的安全指纹认证服务器向客户终端发送指令以在客户终端处获取用户的指纹。响应于客户终端浏览器所显示的指令，用户将其选定的手指放到指纹传感器上，然后安装在客户终端里的指纹获取软件获取数字指纹，例如具有 25 微米（micron）至 70 微米间距分辨率以及 12.5 平方毫米（mm^2）至 25 平方毫米的面积，并且还具有 8 位灰度级的象素图像。

安全指纹认证服务器接收指纹数据，并连同接收 User ID 以及互联网 IP 地址和/或指纹传感器单独编码（MAC 地址）和/或 cookie（cookie 是网络服务器存放到客户终端里的数据，用于网络服务器识别该客户终端）和/或任何唯一码或其他识别特定的个体或者终端的信息（例如，来自客户终端和安全指纹认证服务器之间先前的会话的细节），通过接收以上信息，其使用认证软件将接收的指纹数

据与指纹文件进行比较，该文件是预注册的指纹数据以及用户 ID，个人信息，例如姓名、地址、出生日期、非法记录、驾驶执照、社会保险号，等等，其可以是细节比较和或是快速傅里叶变换比较。

在认证程序的开始，用于相关应用的网络服务器 **214** 从视觉上或者听觉上指示用户将其手指放到指纹获取传感器 **110** 上并且敲击其鼠标键或键盘键以从而启动安全处理器 **114** 中的指纹获取软件。接着将获取的用户指纹数据通过 ISO 处理器 **112** 和客户终端 **200** 的网络浏览器 **210** 以加密格式（例如，使用安全 RSA 加密传输协议 HTTPS）发送到指纹认证服务器 **204** 的网络服务器 **220**。如果获取的数据成功匹配其数据库 **226** 中相应的数据，那么指纹认证服务器 **204** 接着将对客户终端 **200** 和对应用服务器 **202** 确认用户的身份。

以下将参照图 3，描述一个采用了三路认证协议和一次性口令作为哈希（Hash）字符编码序列的典型优选实施例：

- 客户终端 **200** 的网络浏览器 **210** 通过请求访问应用程序 **216** 访问相应的应用服务器 **202** 的网络接口 **214**。
- 应用服务器 **202** 的网络接口 **214** 以登入（LOG-IN）屏幕信息和访问应用程序 **216** 的相关指令作为响应。
- 客户终端 **200** 指示 ISO 处理器 **112** 激活安全处理器 **114**。
- ISO 处理器 **112** 触发安全处理器 **114**。
- 安全处理器 **114** 等候来自指纹传感器 **110** 的指纹数据并且当收到有效数据时，提取指纹数字图案，该图案通过 ISO 处理器 **112** 发送到网络浏览器 **210**。
- 网络浏览器 **210** 将指纹提取图案的加密版连同（或与之共同加密）涉及卡 **100'**和读卡器 **208** 的相关信息发送到认证服务器 **204**，例如用户 ID、客户终端 **200** 的 IP 地址、和/或传感器 **110** 的硬布线 ID 编码（MAC 地址）。

- 认证服务器 **204** 的网络接口 **220**，由以上步骤接收指纹提取图案连同来自客户终端 **200** 的其它信息一起，将这些信息发送到指纹匹配处理器 **222**。
- 在匹配软件 **224** 的控制下，指纹匹配处理器 **222** 使用收到的用户 ID 或者其它的用户特定相关信息，从数据库 **226** 检索相应的指纹参考图案并且将指纹获取图案与指纹参考图案进行比较。
- 将结果（匹配或不匹配）连同对终端 **200**、用户 ID 卡 **100'** 和应用请求 **216** 进行验证的相关信息一起存储到访问历史日志中，并且将控制返回给认证服务器网络接口 **220**。
- 如果结果为匹配，那么认证服务器网络接口 **220** 产生一个形式为询问（challenge）字符序列的一次性密码，其被传输到客户终端 **200**，并且使用询问字符序列作为哈希码，以将相关信息进行加密，其被保存为相应的询问响应，用于可能的将来的参考。
- 客户终端 **200** 使用收到的询问字符序列作为哈希码，以将先前存储的相关提交信息的未加密拷贝进行加密，然后将其发送到应用服务器 **202** 的网络接口 **214**，作为其对应用登入程序的响应的一部分。
- 应用服务器 **202** 的网络接口 **214** 由以上步骤接收经过哈希转换的相关信息，将其发送到应用服务 **216**，该服务将其与来自客户终端的登录（LOG-ON）企图结合，并且，为了确认匹配结果，将收到的相关信息发送，该信息已被客户终端使用由认证服务器提供的询问序列进行哈希转换以作为询问响应。
- 认证服务器 **204** 的网络接口 **220**，由以上步骤接收来自应用服务器的询问响应，将该响应发送到认证处理器 **222**，该处

理器将其与先前保存的预期询问响应的参考拷贝进行比较，以决定用户身份是否事实上已被授权。

- 由该比较产生的任何授权用户身份信息接着通过认证服务器网络接口 **220** 和应用服务器 **202** 的确认接口 **218** 而返回到应用程序 **216**。
- 确认接口 **218** 通过认证以确认在初始登录企图时建立的用户身份已经生效。
- 一旦用户身份被确认，认证（应用）程序 **216** 则通过应用服务器 **202** 的网络接口 **214** 进行与客户终端 **200** 的网络浏览器 **210** 直接通信。

图 6 示出了可选认证程序，其中所有的匹配通过安全 CPU **114** 在图 4 的 ISO 兼容卡上执行，并且没有采用外部认证服务器 **204**。图 6 的左边示出了由应用服务器 **202** 执行的功能，而右边示出了由 ISO 智能卡 **100** 执行的功能。

当将智能卡 **100** 插入读卡器 **208** 时，复位信号 RST 从读卡器发送到 ISO CPU（START 方框 **502**）和指纹 CPU **114**（指纹验证方框 **504**），并且该两部件从读卡器 **208** 接收电源 VCC。然后 ISO CPU 响应以 ATR（Answer-to-Reset 复位应答）消息并如有必要则发出 PPS（Protocol and parameters Selection 协议与参数选择）（方框 **506**）。同时，指纹 CPU 进入等待状态以接收指纹数据，以及当从传感器 **110** 收到数据时，就执行认证程序（方框 **504**）。

当初始请求命令被应用 **216** 发送到 ISO CPU **112**（方框 **508**）时，ISO CPU 向安全 CPU 询问（方框 **510**）认证状态。如果响应为肯定，那么 ISO CPU 通过运行请求命令以响应应用（方框 **512**）。否则（来自安全 CPU **114** 的不管是错误信息还是没有响应）其不对请求命令做任何响应，而是等待新的第一请求（方框 **508b**）。

假定指纹被验证并且第一响应被及时收到且其被应用 **216** 确定是响应信号（方框 **514**），那么请求/响应程序将将一直持续（方框 **516**、**518**、**520**）到超出预定验证时限，在此期间不从该应用接收请求（方框 **522**），或者该应用不能接收预期响应（方框 **524**）。

图 7 类似于图 6 的流程图，但是修改为采用了图 5 的典型生物验证卡。图 7 的最左边示出了由应用服务器 **202** 执行的功能，下一列对应于读卡器 **208**，再下一列描绘了 ISO 触点 **108**，又下一列示出了由安全 CPU **114** 执行的功能，而最右边则示出了由无变更 ISO 智能卡 **112** 执行的功能。

- 当将智能卡插入读卡器时或者应用软件开始运行读卡器设备时，将复位信号 **550** 从读卡器 **208** 发送到安全 CPU **114**。
- 安全 CPU 收到复位信号 **550** 之后不久，其发送相应的复位信号 **552** 到 ISO CPU **112**。同时安全 CPU 等待来自指纹传感器的指纹数据。
- 由以上步骤收到复位信号 **552**，ISO CPU 产生 ATR（Answer-to-Reset）响应 **554** 并此后如有必要则发出 PPS（Protocol and parameters Selection）。
- 安全 CPU **114** 一旦从 ISO CPU 收到 ATR(Answer-to-Reset)，就立即将其，包括任何相关的 PPS 命令，传输到读卡器（方框 **556**）。
- 同时，如果安全 CPU 收到指纹数据，那么其将执行前面描述的认证程序。在认证检测结果为 PASS 的情况下，该通过状态将维持一定的时间周期。如果结果为 FAIL，那么安全 CPU **114** 就等候新的指纹数据。
- 由以上步骤运行该应用，将命令请求 **558** 发送到安全 CPU，只有在安全 CPU 仍然处于前面描述的 PASS 状态时或最后的正确响应具有多数据位组时，该安全 CPU 才将命令请求

560 发送到 ISO CPU 并还将其正确响应 **562** 发送到读卡器（检测方框 **564**）。

- 否则（No 分支 **566**）指纹 CPU 产生伪请求（dummy request，虚拟请求）**568** 并将其发送到 ISO CPU 并还将该结果 ERR 响应 **570** 发送到读卡器 **216**，从而在请求中的序列号与响应中的序列号之间保持正确同步。

加密和保密

在通过任何外部网络进行传输之前，优选地，将任何敏感数据和/或认证结果都进行加密，可采用 DES、或 Two Fish 加密。加密密钥可以基于指纹获取或存储数据、用户 ID 编码、传感器的唯一分配编码、存储器地址、存储器里邻近的数据、其它功能上相关的数据、先前的会话（事务处理）、IP 地址、终端编码、或者指定的口令。可选地，敏感数据可以使用安全 HTTPS 协议以通过互联网发送。

为了提供更强的安全性，可以将虚拟个人网关，例如硬件 DES 加密和解密，插入安全指纹认证服务器与网络连接之间，以及相应的应用服务器与网络连接之间。通过这样来使用这些虚拟网关或者虚拟专用网络（“VPN”），将敏感数据通过附加的加密层进行附加保护，例如 DES **128**（通常用于 VPN）和 RSA（被 HTTPS 采用）。

为了特别安全的应用，所有的通信可以用附加的保密层来包围。特别地，较低层中的报文头可以在较高层中进行加密。

无线通信

其它实施例可以包括用于既接触（ISO 7816）操作又无线（ISO 1443 A 或 B）操作的双重接口，并且优选地，安装有多接口电源单

元，其允许在全部在一张卡上的 ISO 7816 接触、ISO 1443 A、ISO 1443 B、ISO 15693 和 HID 传统无线系统（在其它的之间）之间互用。可选地，卡可包括用于其它无线通信技术的备用件，例如蓝牙（短距离）或者蜂窝（中距离）或者微波（长距离）。

接下来参照图 8，其示出了具有可无线或者借助于电接插件连接到本地终端的卡上生物验证的智能卡。其大部分结构和构造相似于前面描述的图 1 的实施例，并且同样的标号（可能以单引号加以区分）标示相似的元件。特别地，ISO CPU **112** 虽然显示在不同的位置（在触点 **108** 下面，而不是一侧），但是有如前所述的相似功能。

ISO 天线 **132** 包括通常设置在卡 **100** 的周边的两个环状天线，并且向 ISO CPU **112** 提供 ISO 兼容无线接口，用于使数据和功率相似于有线电接口 **108** 所提供的数据和功率。另外，安全天线 **134**（在所述例子中，内置天线 **132** 且只由一个环状天线构成）通过 DC-DC 功率调节器 **120** 向安全 CPU **114** 提供独立的电源。因为除了通过 ISO CPU **112** 没有用于无线数据的直接连接，所以存储在安全 CPU **114** 内的敏感数据不被该无线接口破坏。可选地，如前所述的关于对外部读卡器和外部网络只有有线连接的实施例，两个处理器的功能可以被合并，或者外部接口可以是通过安全 CPU **114** 而不是通过 ISO CPU **112**，其中必须将适当的无线安全措施结合到该变体构造中。

图 9 是图 8 所示的卡的截面图。注意到大多数所述元件包含在芯区 **126** 中，只有触点 **108** 延伸物穿过上保护层 **122**。传感器 **110** 的操作面通过上层 **122** 中的上窗口和 PCB（印刷电路板）**134** 中的下窗口以可访问，该 PCB **134** 被布置在上层 **122** 和中心层 **126** 之间，其提供各种电子元件之间必需的电连接，以及围绕传感器 **110** 有效区域的环绕的静电放电接地连接。

下层 **124** 和磁条 **128** 仍是可见的。

指纹传感器

图 10 是传感器 **110** 的典型示意电路图，其中传感器单元 **402** 阵列 **400** 排列为行 **404** 和列 **406**。如上所述，每个单元 **402** 包括激活门 **410** 和变换器 **412**。指纹由手指上皮肤的凸部和凹部形成。当这些凸部之中的一个触及阵列 **400** 内单元 **402** 的附近时，每个传感器单元的变换器 **412** 经历一个机械的和/或电的变化，其实际上产生了基于传感器表面上的由指尖上凸部和凹部引起的微压变化的指纹数字图像。注意到尽管每个变换器 **412** 被描述为单个可变电容器，但是有各种类型的变换器可以响应人类皮肤的这些凸部之中的一个的出现。在压力传感器压电薄膜变换器的特别实例中，该薄膜在单元的附近变形并且产生存储在连接到该单元的电容器中的电荷。电容器上的电压是由压电材料的变形形成的机械应力的函数，其进而是在单元上是凸部还是凹部的函数。当来自相关列驱动 **414** 的信号将该单元的门 **410** 达到 ON 时以及当相关行驱动 **416** 被接地时，电压出现在行的输出线路 **418** 上，并且在输出驱动 **420** 中转换成 8 位数字信号。为了最大化地探测压电材料的变形，压电电气材料可以在弹性材料上形成，例如聚酰亚胺或者聚酰亚胺压电电气材料即可。其它典型的可以用类似的阵列组织实现的模拟变换器技术包括可变电阻和可变电容器。可选地，每个单元可以包括简单的数字开关，其仅仅提供单比特信息；在此情况下，信息的附加的位可以由在同一区上提供多个单元或者由以更高的频率抽样每个单元来产生。该可选实施例避免了对 A/D 转换器的需要。

在典型实施例中，传感器只有 0.33 毫米厚并且足够坚固以嵌入到智能卡中并且不受静电、元件或者用户皮肤状态（湿、干、热、冷）的影响。传感器 **110** 通常的装置单元尺寸是 25 微米至 70 微米并且通常的间距是 25 微米至 70 微米。典型传感器具有 12.5 平方毫

米至25平方毫米的面积以及8位多级灵敏度。该传感器可以由TFT（薄膜晶体管）和压感电容器阵列制成，例如由薄膜压电材料形成，例如钛钡氧化物或者锶钡氧化物，并且包括上电极，其覆盖并且保护整个传感区域。如果采用机械应力，那么将产生相应的电荷并且存储在薄膜压电电容器中。可选地，基于压力的传感器可制成TFT（薄膜晶体管）连同薄膜电容器，以及压感电容器的阵列，例如由压力传导材料片形成，例如碳化纤维分散橡胶片，金属（例如铜或锡或银），电镀的碳化纤维或纸底基玻璃纤维或金属，分散弹性材料（例如硅树脂）以及覆盖整个传感区的上电极片。

指纹传感器元件**402**特别规定的行和列驱动**416**、**414**输出电数据到输出电路**420**，从而将表示用户指纹的物理输入转换为模拟电数据。然后输出电路**420**中的A/D转换器将该模拟电信号转换为数字电信号。每个薄膜晶体管选择性地将共享的行间互连转换为其相关的电容器上的电压，这样每个电容器上的电压可以被读取并且因此每个单元的变形可以被测量。优选地，薄膜晶体管的整个列被同时转换，从而在一个选定列中的多个单元（例如8个）可以在不同的行间互连上被并行读取。多个门如行和列间的互连减少了互连的数量，而从相同列的不同行并行读取多个单元则减少了整个阵列的读取时间时，。来自传感器的输出电压可以由差动放大器放大。可以将该放大器的输出采样和保持用于A/D转换器。

基片可以是玻璃（例如非碱性玻璃）、不锈钢、铝、陶瓷（例如氧化铝）、纸、玻璃钢，但优选是晶体硅薄板。薄膜半导体材料可以是无定形硅、多晶硅、金刚石、或者任何其它半导体薄膜。压电材料可以是压电陶瓷，例如铅－锆酸盐－钛酸盐（lead-zirconate-titanate，PZT）薄膜，优选地，厚度范围为0.1至50.0微米，或聚合物压电聚酰亚胺薄膜材料。互连材料可以是：钛/镍/铜、铝、铬/镍/金、钛/镍/金、铝/金、钨/铜、钨/金、钨/金。

图 11 示出了形成在晶体硅的薄基卡上的传感器的载体组合。晶体硅具有极好的电气性质并且有利于将传感器阵列与所需驱动和输出电路集成，然而在相对大而薄的硅薄板受到局部表面压力时将会弯曲和断裂。图示的载体提供了比同样整体厚度的硅片更结实的结构。

如图所示，单片硅 **430** 大约 0.1 毫米厚，并且由相同厚度的玻璃钢框 **432** 围绕，其被安装在也是玻璃钢结构的垫板 **434** 上并且约 0.05 毫米厚。框 **432** 和垫板 **434** 可以很容易地使用传统的印刷电路板（PCB）技术来构造。特别地，垫板 **434** 的上和下表面由被玻璃钢芯分隔的薄铜层 **436** 所覆盖。框 **432** 包括多个在其外部边缘的焊盘 **440**，用于连接到安全处理器 **114**。薄硅片 **430** 用环氧树脂粘合到框 **432** 和板 **434**，并且有效区由在围绕着受保护的上电极 **446** 的硅 **430** 的暴露的外边缘部 **444** 上的传统的布线连接 **442**，电连接到框 **430** 中各自的电路。

匹配算法

对于处理能力有限并仅试图与单一参考样本做简单的 1:1 匹配的本地卡上处理，指纹匹配软件可以是基于两个图案的细节的相对简单的比较。例如，指纹的灰度图像可以被减小到两个值，白和黑，并且三维凸部被转换成二维细线（矢量）。因而，该方法的准确性还受到以下问题：模糊、粘连、失真、线段部分缺失和其它的影响。尽管细节方法理论上正确率较低，但其需要较少的计算资源并且提供与许多现有数据库兼容的可能性。

对于在具有更强处理能力的远程认证服务器上进行处理，可以要求更高的准确分辨率，例如“POC”（Phase Only Correlation 仅相位对比）匹配算法。POC 是基于整个图像的宏匹配的验证算法。相反地，POC 匹配大范围的结构信息－从细节到总图像。因此，POC

能够提供加强的准确度来避免噪声，例如粘连和部分缺失。理论上，POC 方法不受来自位置移动和亮度差异的不利影响，并且快速（对于脱机匹配约为 0.1 秒）和高准确度。例如，POC 软件可以利用二维快速傅立叶变换（“2DFFT”）来执行两个指纹图案的空间频率比较。2DFFT 将表示指纹的物理二维分布的数字化数据阵列转换为频率空间，换句话说，将空间分布反转换，该处越高的密度图案具有越高的空间频率。旋转变换可用于对频率空间图案匹配进行匹配。因为不被指纹记录图案中的普通缺陷误导，POC 将认为这些缺陷为噪音而细节分析将这些缺陷作为有意义的数据进行解释，所以 POC 图案匹配与细节向量匹配相比有更多的优点。

对于特别苛刻的应用，混合方法将可比其它任何单独的方法提供更高的准确度和安全性。例如，细节方法可以用在获取点上，而 POC 方法可以用在远程服务器上。作为另一个例子，匹配程序可以分析细节和空间关系以产生考虑了两种结果的结合的分数。

应用

前面描述的技术提供了用于多样的应用，商用的和政府的，高水平的安全性。根据各种应用的要求，多种安全应用可以共存并在相同的卡上和/或相同的认证服务器上操作。在一个实施例中，单张卡可以包括多至 24 项独立的且安全的应用。例如，该技术将许可/拒绝访问（物理的和/或逻辑的），识别人员的精确位置和/或运动和/或监视列出的名单，而且同时还运行其它安全应用，各应用相互间完全地且安全地隔离。

当前可以预期的应用如下：

- 机场 ID/通行
- 大厦保安

- 旅馆房间通行和记帐
- 医院
- 在线游戏
- 下载娱乐
- 出生证明
- 计算机访问
- 驾驶执照 - TWIC
- 电子钱包
- 紧急医学信息
- 炸药执照
- 政府和军用设施通行
- HAZMAT（危险物）许可证
- 医疗保险和福利卡
- 停车场入口
- 护照
- 航空执照
- 港口 ID/通行
- 保险证明
- 社会保险卡
- 旅行信用卡
- 签证或者进/出通行证
- 投票注册卡
- 福利和粮票印花卡

对于许多的这些应用，优选地，卡的卡上存储器还提供各种私人信息的安全存储，其只有当注册的持卡人证明了其身份和授权该访问时才可进行访问。这些私人信息的实例有：

- 管理信息，例如姓名、地址、出生日期、出生地点、国籍、宗教、组织关系、社会保险号码、驾驶执照号码、护照号码、和移民信息例如签证类型、签证期限、国籍等。
- 财务信息，例如电子钱包、VISA（VISA 信用卡），MasterCard（万事达信用卡），American Express（美国运通信用卡）等信用卡信息，银行信息，例如银行名称、银行存款余额、转帐信息、IRS（美国国税局）号码、破产记录、转帐信息等。
- 体征和健康信息，例如：识别个人的生物信息，例如身高、体重、指纹、虹膜、视网膜、手尺寸、骨结构、声音、DNA；血型；医学诊断检测结果；病史；药物；保险信息；对一定刺激的心理和生理反应等。
- 事件信息，例如犯罪记录、重罪、轻罪、违法。
- 应急信息，例如墓地、亲属和其它联系信息、律师信息、宗教信息。
- 教育、工作历史，包括学校、学位、就职过的与 FDD 有关的公司。
- 数据访问历史（存储了进卡和出卡的访问历史数据）。
- ID 相关信息，例如指纹图案、指纹处理图案、指纹图案的结果。
- 口令，例如永久口令、暂时口令、和/或一次性口令。
- 加密密钥，例如公开密钥、个人密钥、和/或一次性密钥。

接下来描述典型的卡注册系统。

申请人：填写申请表并且将其提交，优选地，包括照片和指纹。对于大部分申请人，检查其文件附件并简单地在一个或多个政府和商业数据库中查对提交的信息就足以建立个人的真实身份。

在其身份被识别后，申请人进入签发站，此处由发卡人将认为必要的任何信息载入卡中。申请人将其手指放在卡上的传感器上。一旦指纹符合要求地置于传感器上并且被载入卡中，就将使卡上的突出受到电冲击，其烧断某些保险丝，以阻止任何人再次写入卡的该一定区域。然后，将该小突出切断/剪断（就像带有脐带的卡）。在该点处，卡只能通过 ISO 接触读卡器或者 ISO 无线系统进行读或者写。

在网络认证服务器的情况中，卡上所载同样数据的一些或者全部也是以加密形式传输到远程服务器，可以补充附加的通常不存储在卡上但是可能需要用于高安全性应用的数据。

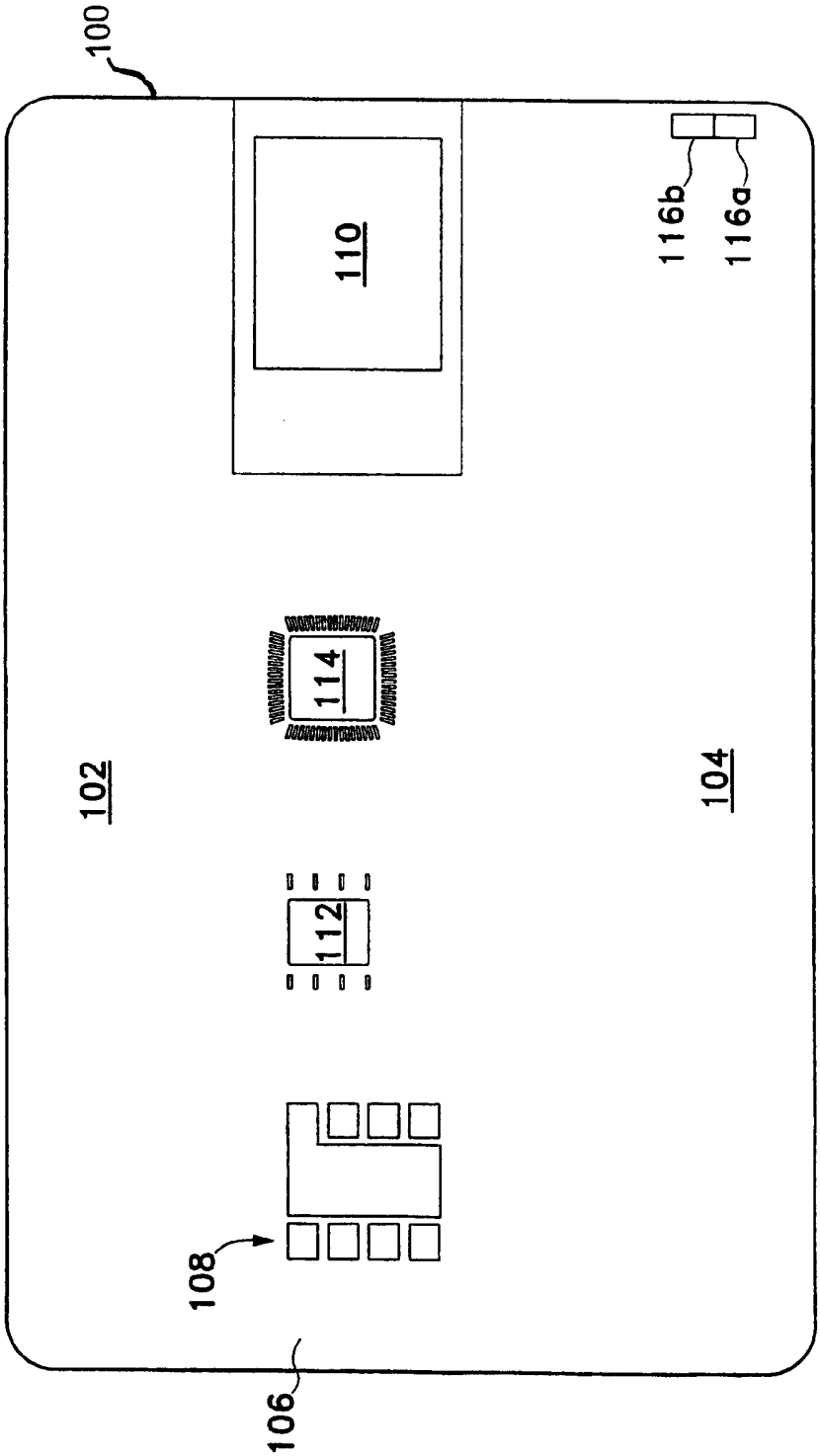


图 1

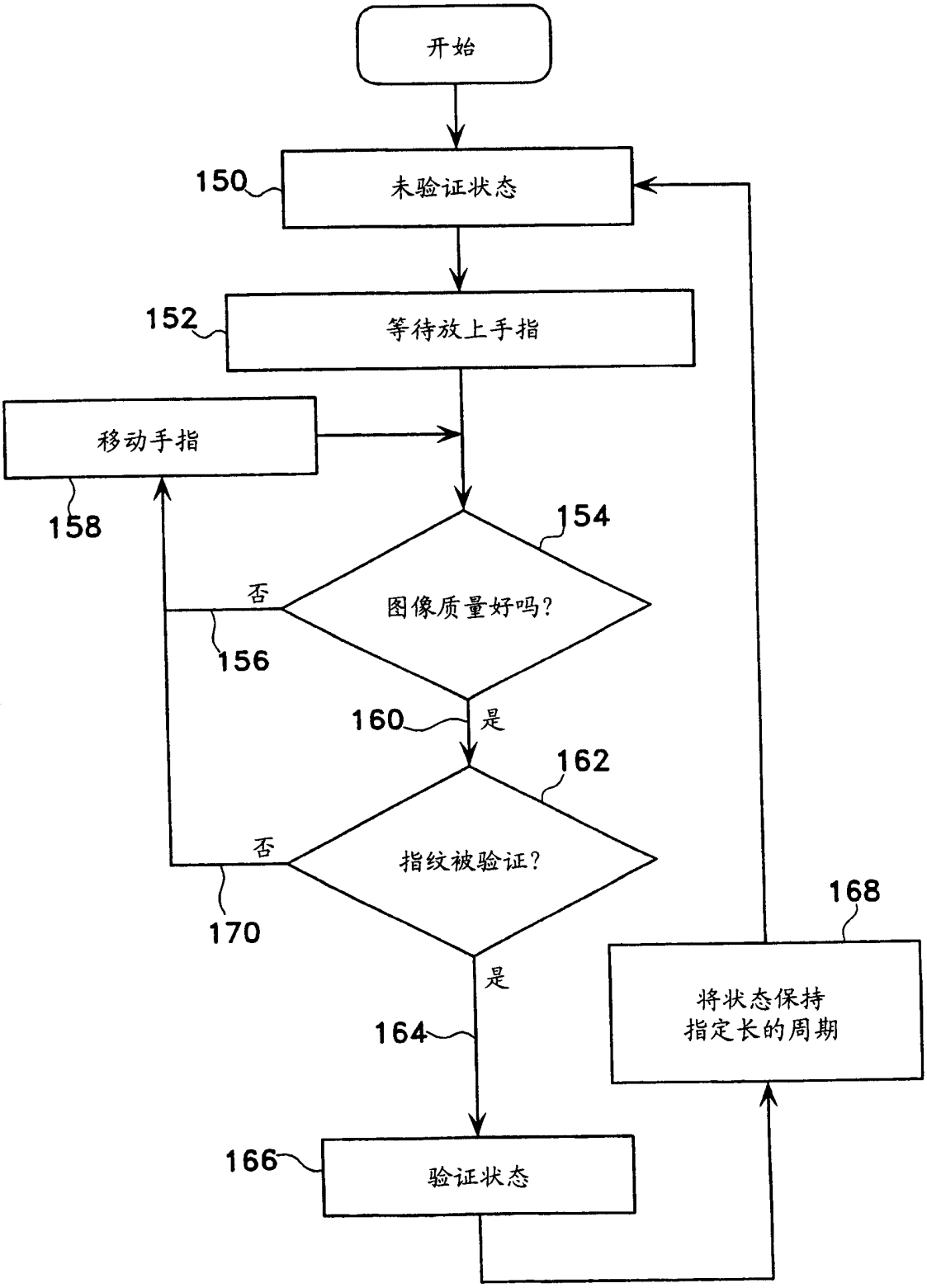

开始
150
未验证状态
152
等待放上手指
移动手指
158
154
否
图像质量好吗?
156
160
是
162
否
指纹被验证?
170
是
164
168
将状态保持
指定长的周期
166
验证状态

图 2

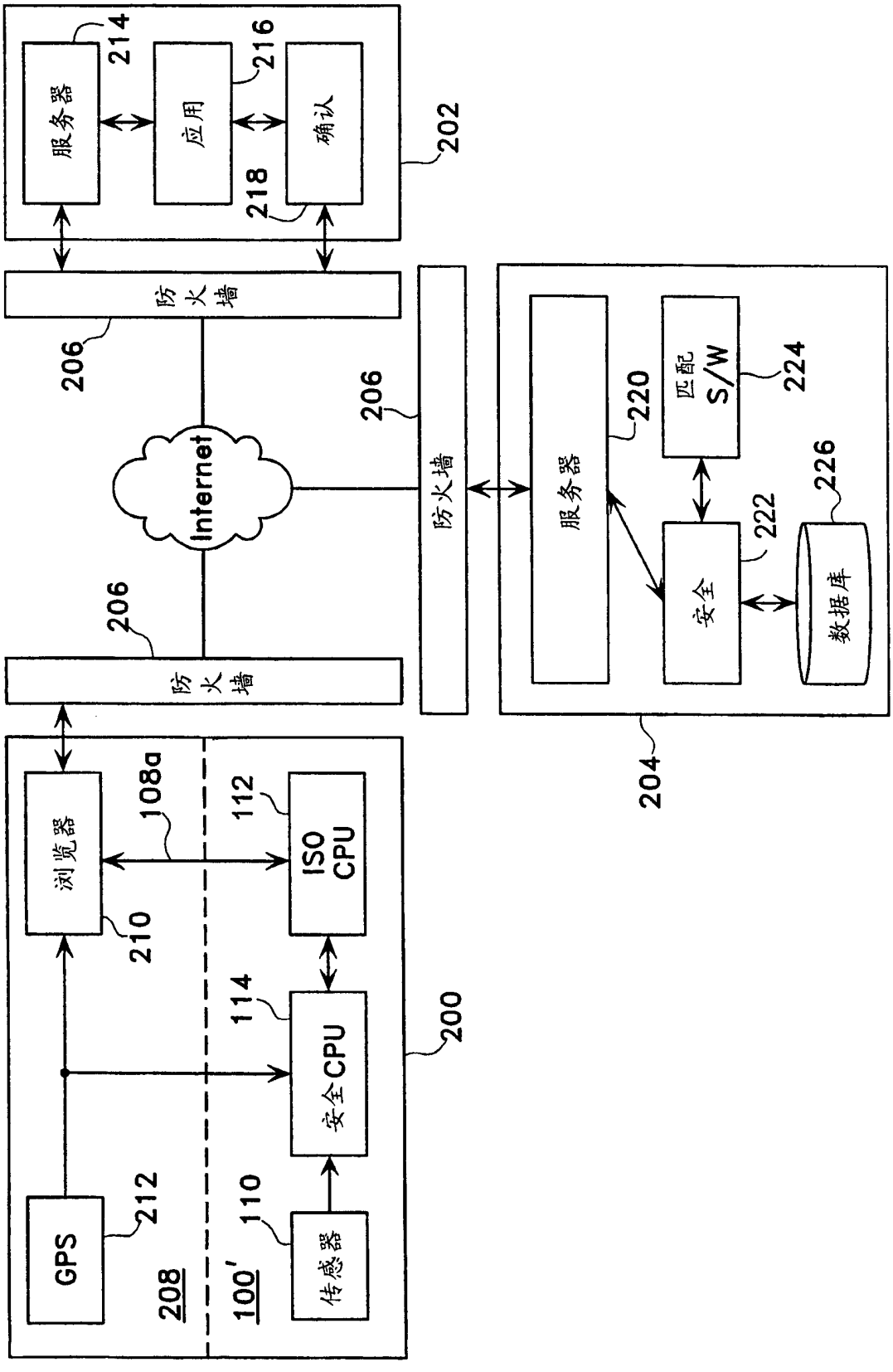

服务器
214
应用
216
确认
218
202
防火墙
206
Internet
206
防火墙
206
防火墙
服务器
220
匹配
S/W
224
安全
222
数据库
226
204
浏览器
108a
112
ISO
CPU
210
114
安全CPU
200
GPS
212
208
100'
110
传感器

图 3

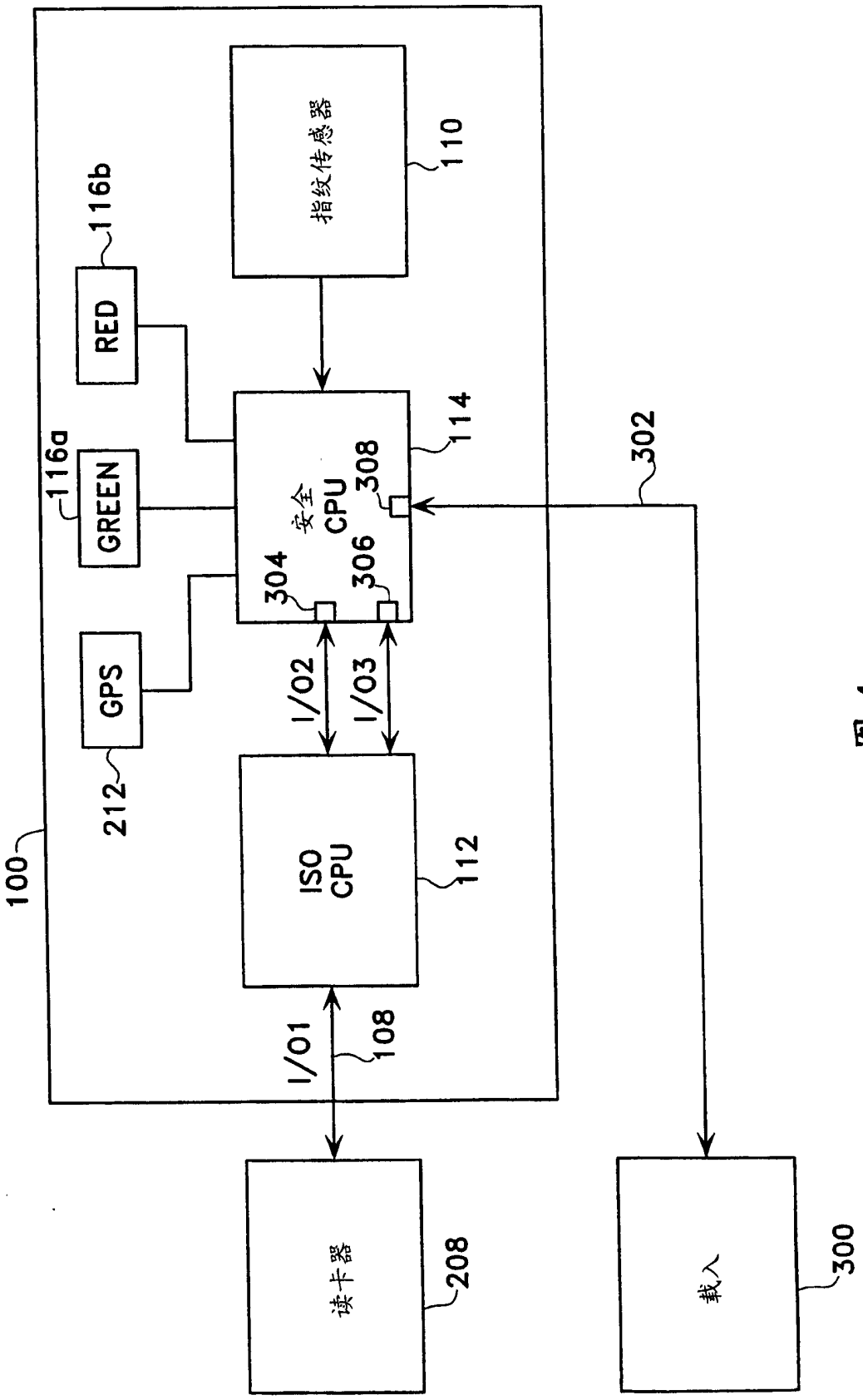

100
指纹传感器
110
116b
RED
116a
GREEN
GPS
212
114
安全
CPU
308
304
306
I/02
I/03
ISO
CPU
112
I/01
108
302
读卡器
208
载入
300

图 4

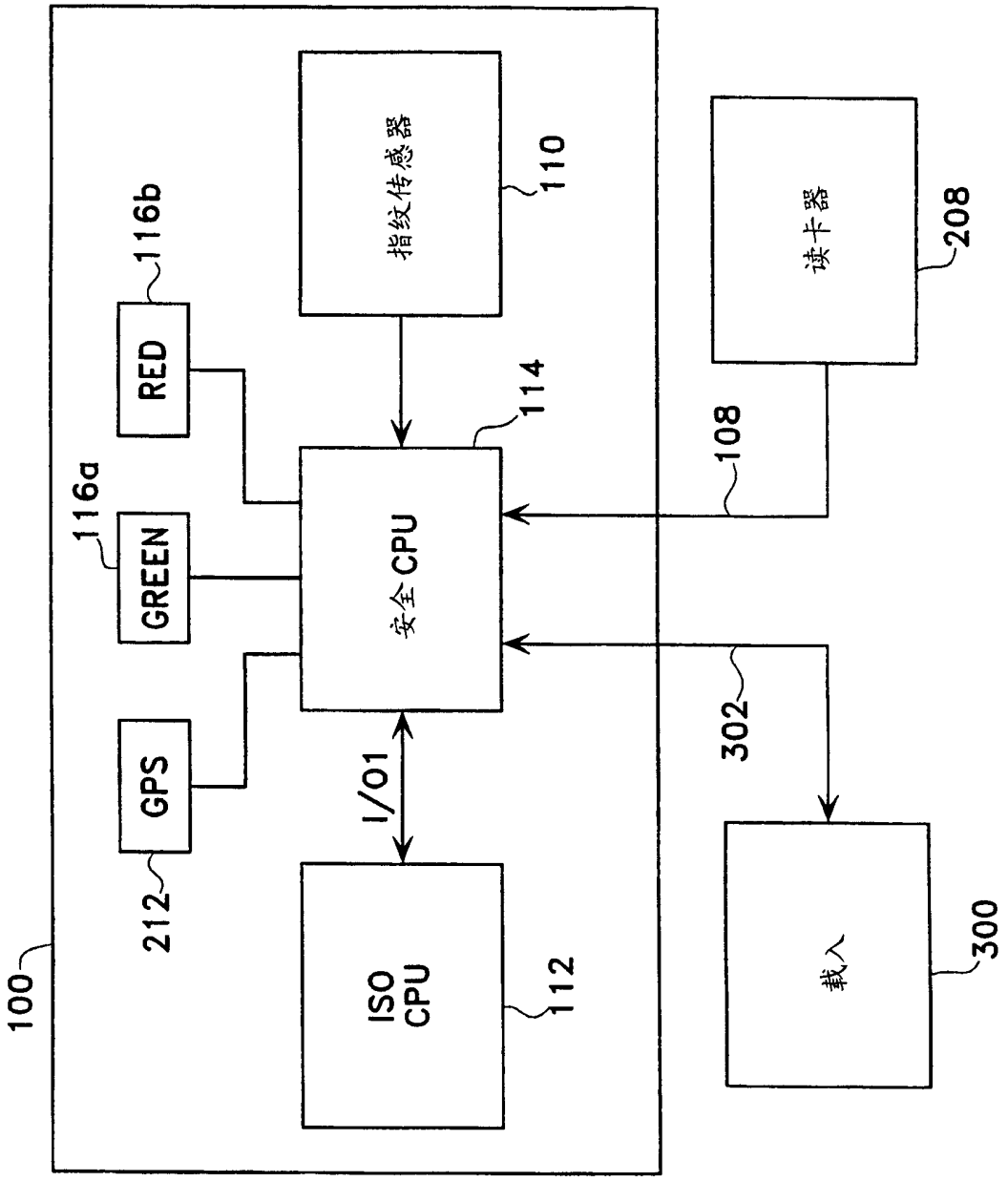

100
指纹传感器
110
读卡器
208
116b
RED
116a
GREEN
GPS
212
安全CPU
114
108
I/O1
302
ISO
CPU
112
载入
300

图 5

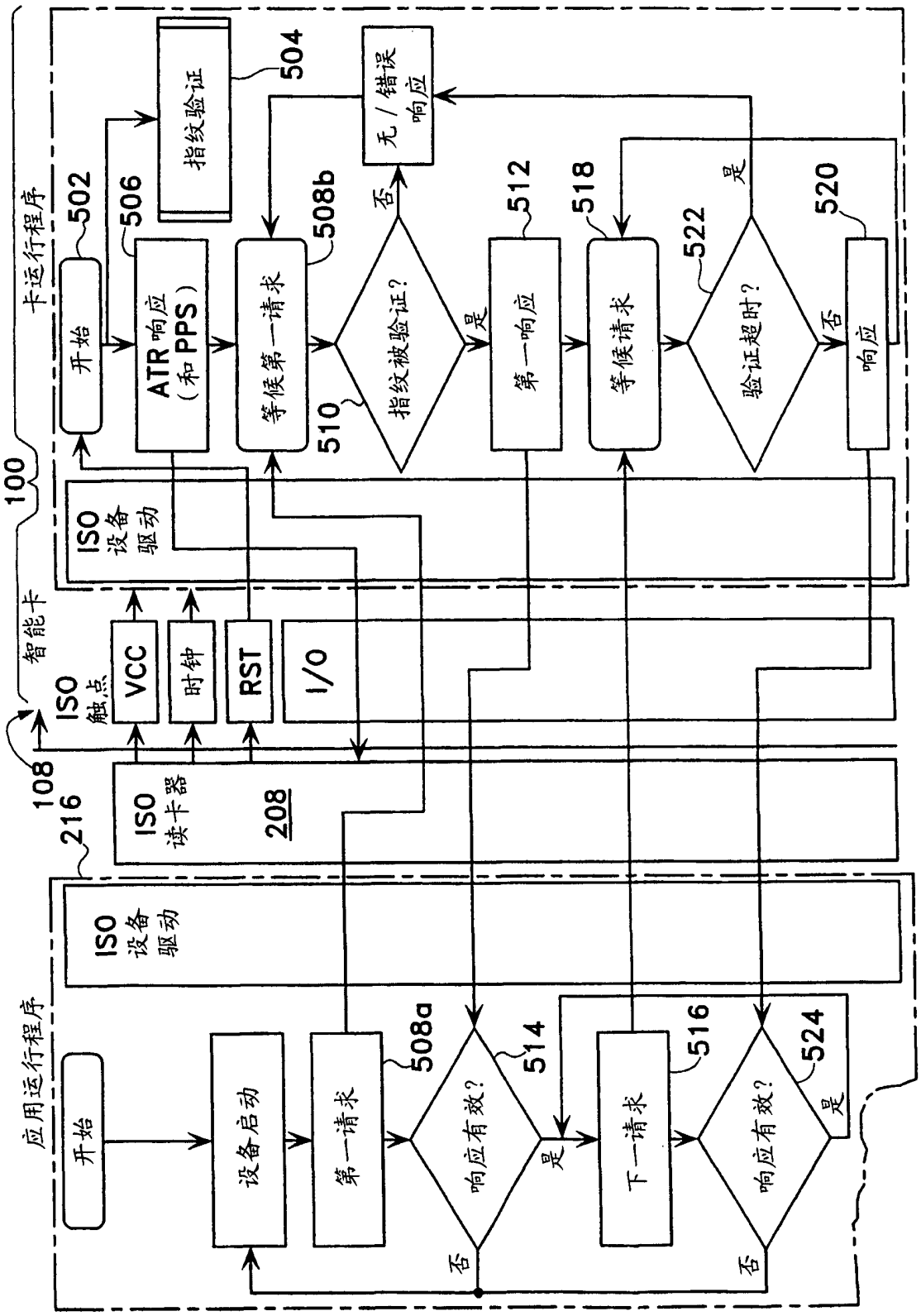

应用运行程序
开始
设备启动
第一请求
508a
响应有效?
514
否
是
下一请求
516
响应有效?
524
否
是
ISO 设备驱动
ISO 读卡器
208
216
108
ISO 触点
VCC
时钟
RST
I/O
智能卡
100
卡运行程序
ISO 设备驱动
开始
502
ATR 响应 (和 PPS)
506
指纹验证
504
等候第一请求
508b
指纹被验证?
510
否
无 / 错误响应
是
第一响应
512
等候请求
518
验证超时?
522
是
响应
520
否

图 6

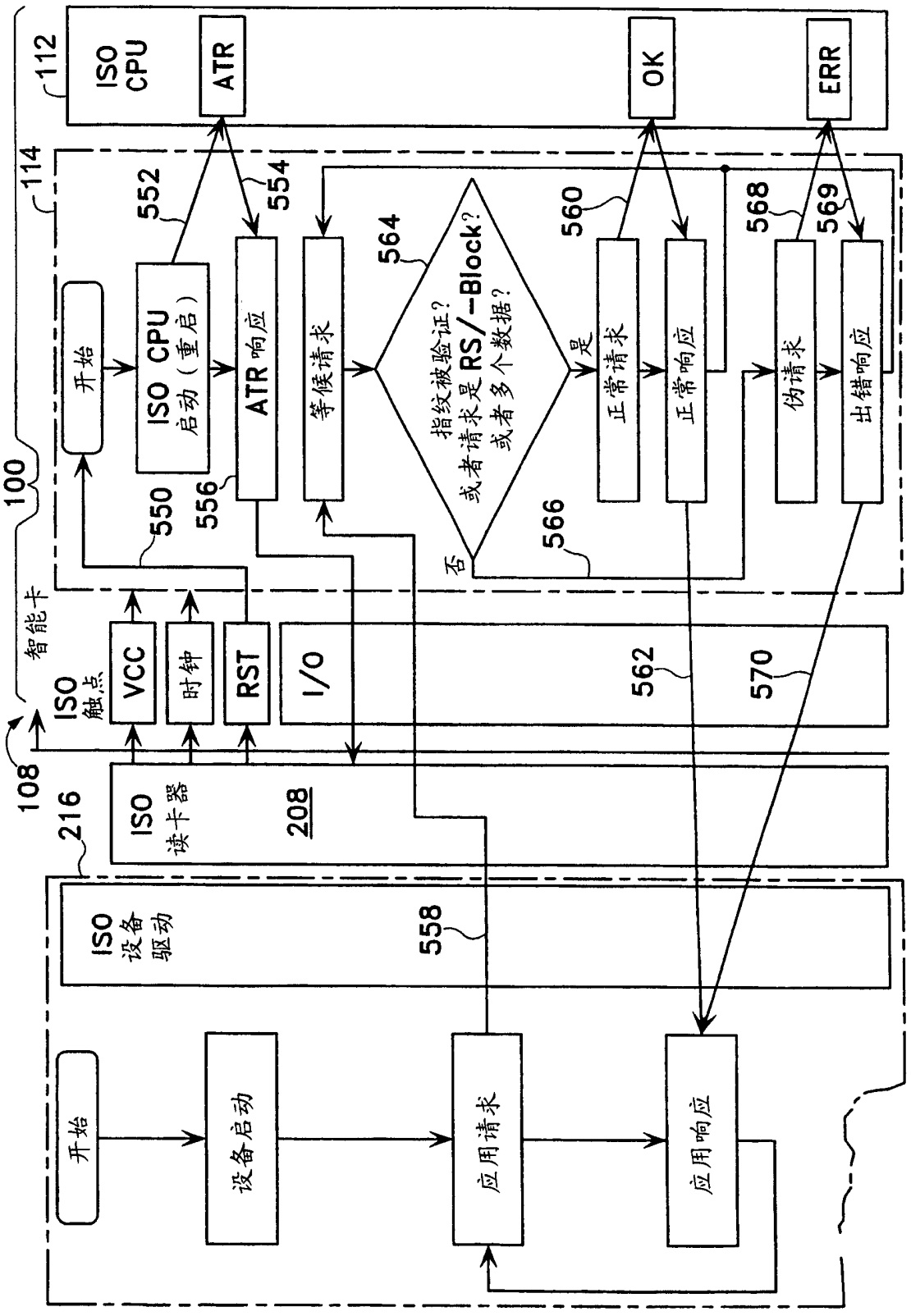

ISO CPU
112
ATR
OK
ERR
114
552
554
564
560
568
569
开始
ISO CPU 启动（重启）
ATR 响应
等候请求
指纹被验证？
或者请求是 RS/-Block？
或者多个数据？
正常请求
正常响应
伪请求
出错响应
是
否
100
550
556
566
智能卡
ISO 触点
VCC
时钟
RST
I/O
562
570
108
216
ISO 读卡器
208
ISO 设备驱动
558
开始
设备启动
应用请求
应用响应

图 7

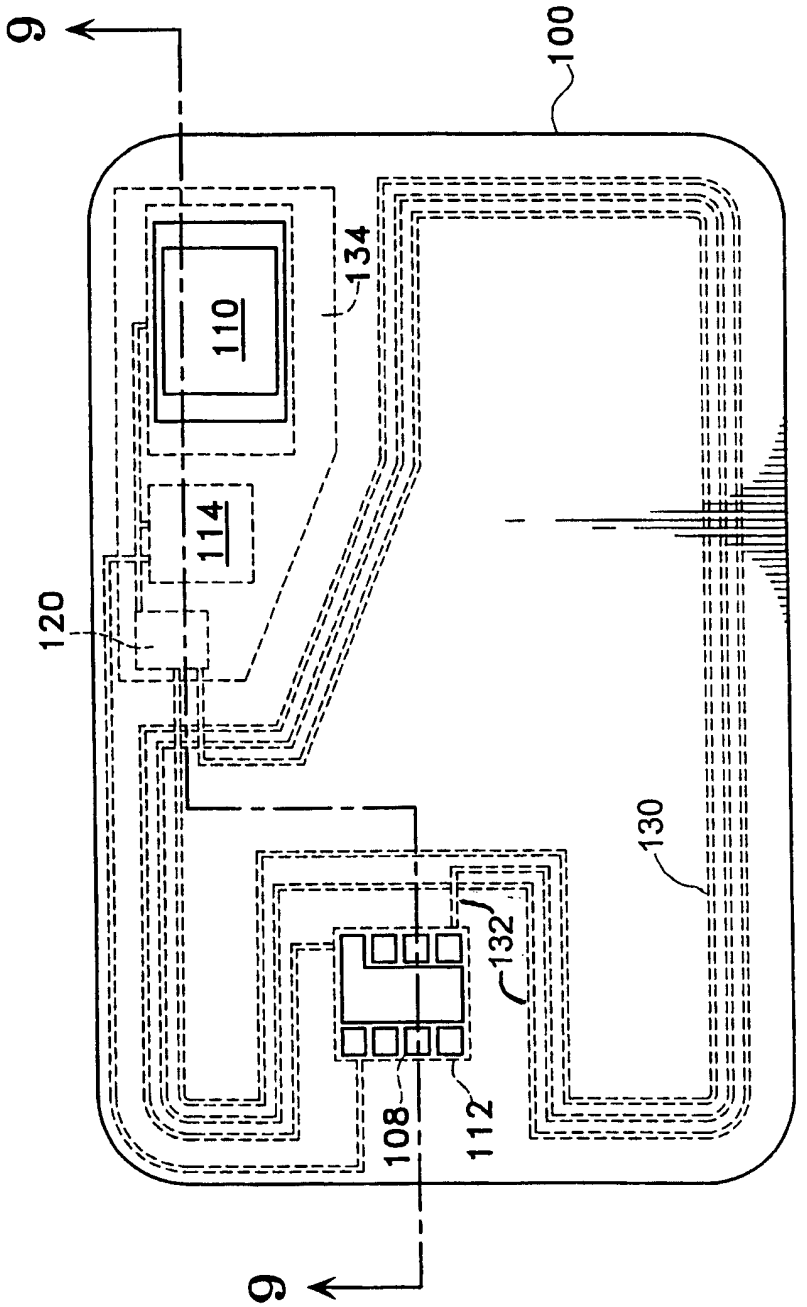

9
100
110
134
114
120
130
132
108
112
9

图 8

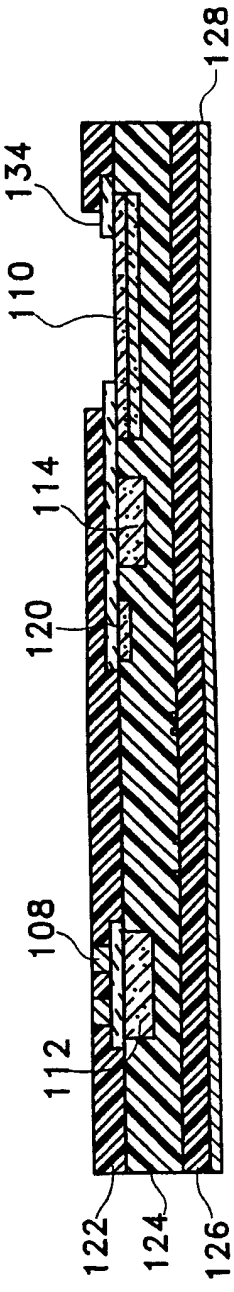

128
134
110
114
120
108
112
122
124
126

图 9

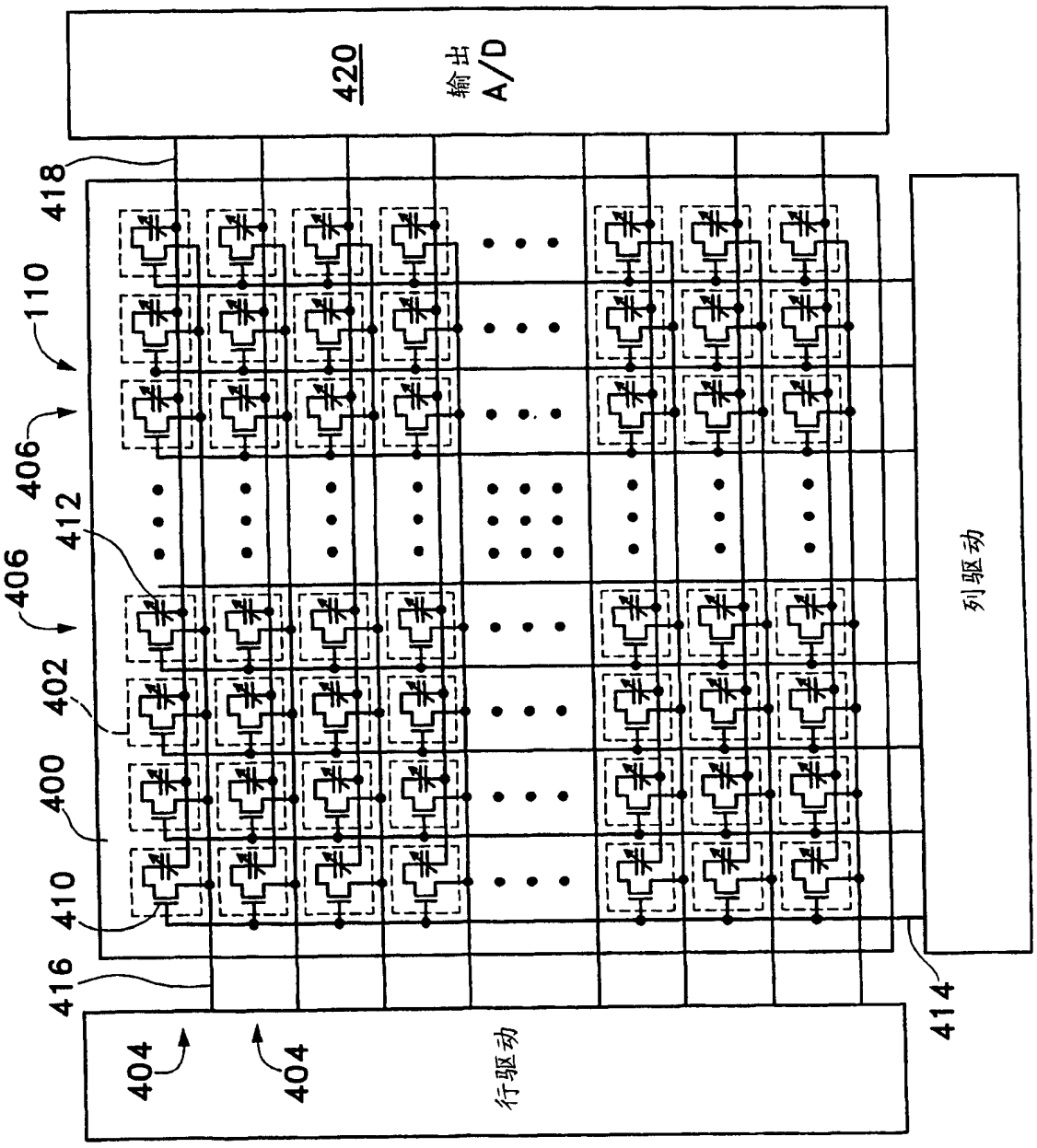

420
输出
A/D
418
110
406
406
412
406
402
400
410
416
404
404
行驱动
414
列驱动

图 10

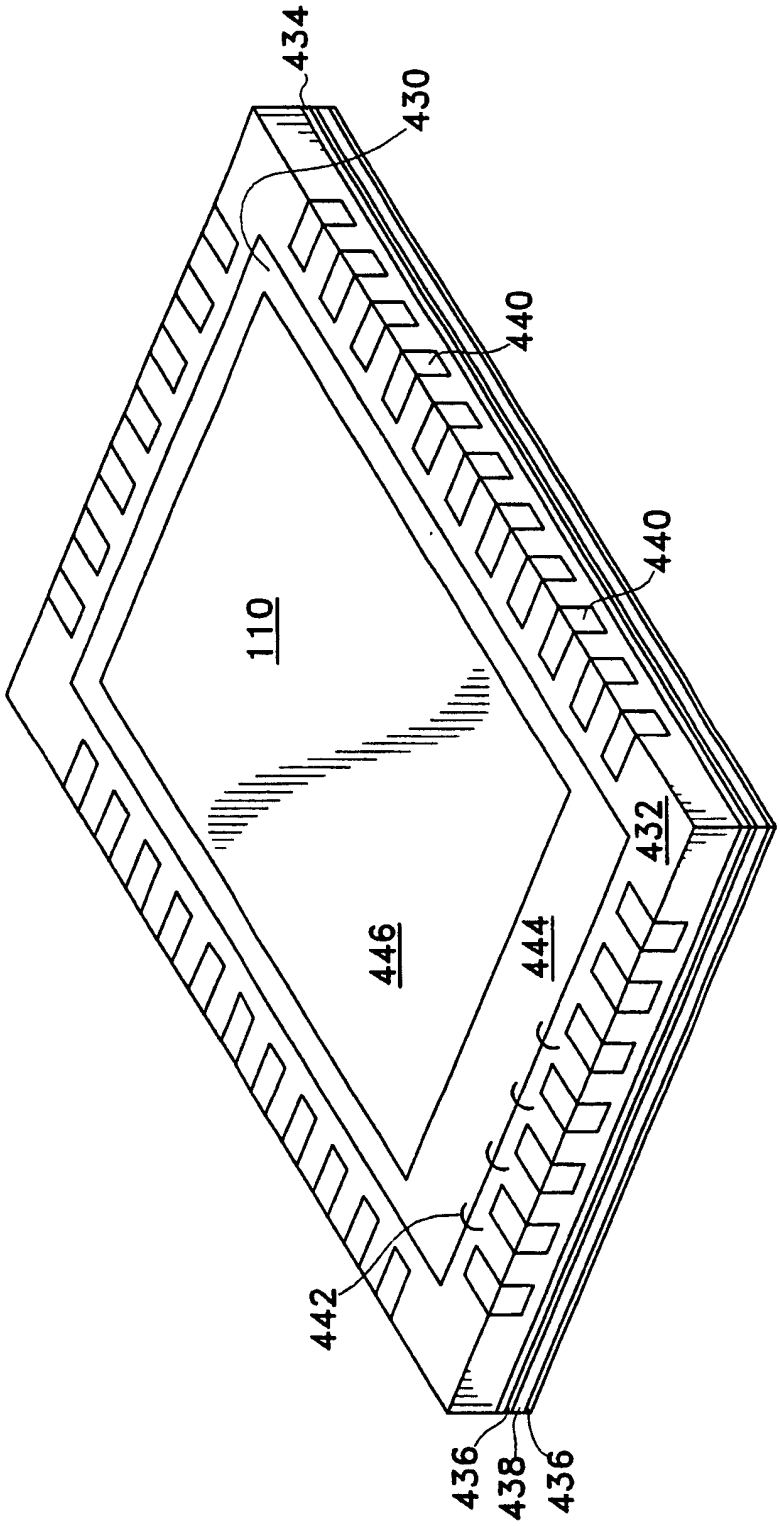


图 11