[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 9/32
G06K 9/00

[12] 发明专利说明书

[21] ZL 专利号 95197455.6

[43] 授权公告日 2003 年 4 月 30 日

[11] 授权公告号 CN 1107395C

[22] 申请日 1995.12.4 [21] 申请号 95197455.6
[30] 优先权
[32] 1994.12.5 [33] US [31] 349688
[86] 国际申请 PCT/US95/15665 1995.12.4
[87] 国际公布 WO96/18168 英 1996.6.13
[85] 进入国家阶段日期 1997.7.24
[71] 专利权人 小查尔斯 A·博格希恩
地址 美国罗德岛州
[72] 发明人 小查尔斯 A·博格希恩
[56] 参考文献
US4805223A 1989.02.14 G06K9/00
US4811408A 1989.03.07 G06K9/00
US4993068A 1991.02.12 H04K1/00
审查员 马红梅

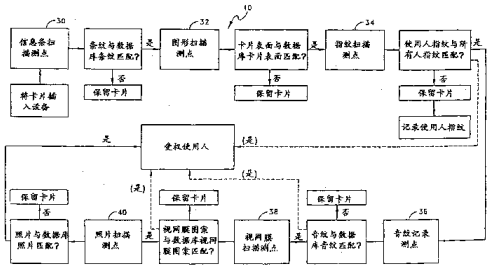
[74] 专利代理机构 中国专利代理(香港)有限公司
代理人 邹光新 王忠忠

权利要求书 2 页 说明书 8 页 附图 3 页

[54] 发明名称 确认具有未授权用户物理特征记录的信用卡的使用的系统

[57] 摘要

本发明涉及确认信用/标识卡(12)授权使用人的方法和设备(10)。 方法包括以下步骤：利用具有数个用于扫描条形码(16)的扫描装置的设备扫描卡片(12)；扫描卡片(12)以获得窜改痕迹；至少扫描卡片(12)上的一个指纹(18)，及任何其它可检测信息；和比较卡片(12)上的扫描信息和至少存储在一个与设备(10)通信的可访问数据库(44)中所有人信息。 在设备(10)和数据库(44)间数据通信受加密系统(63)的保护。 如果卡片(12)上的信息与存储在数据库(44)中卡片所有人的信息不匹配，那嫉卡片(12)被扣留。 否则，卡片(12)使用人可以自由地把它用于预定目的。



ISSN1008-4274

1.一种电子确认尝试以电子方式得到对计算机系统的访问的个人身份的方法，包括以下步骤：

在所述计算机系统上获取分配给帐户所有人的标识码；

查找存储在与所述计算机系统通信的数据库中的所述所有人的信息档案，利用所述标识码查找所述信息档案；

获取所述个人的物理特征图象；

比较所获取的所述个人的图象和存储在该帐户所有人的信息档案中的、相应的所述帐户的所述所有人物理特征图象，以把所述个人正确地识别为该标识码的所有人，依据个人图象和相应的所有人图象的匹配情况，所述使用人被授权得以对所述计算机系统访问；和

在个人物理特征图象与存储在帐户所有人信息档案中的、相应的标识码所有人物理特征图象不匹配的情况下，记录该个人图象。

2.根据权利要求1的方法，还包括这样的步骤：比较所述个人物理特征的所述记录图像和存储在第二数据库中的一组其他个人物理特征图像，试图识别出所述个人。

3.根据权利要求1的方法，其特征在于获取使用人物理特征图象的所述步骤包括获取使用人指纹的扫描图象。

4.根据权利要求1的方法，其特征在于获取使用人物理特征图象的所述步骤包括获取使用人视网膜图案的扫描图象。

5.根据权利要求1的方法，其特征在于获取使用人物理特征图象的所述步骤包括获取使用人的音纹。

6.根据权利要求1的方法，其特征在于获取使用人物理特征图象的步骤包括获取使用人面部特征的照片图象。

7.根据权利要求2的方法，其特征在于获取使用人物理特征图象的步骤包括以下步骤：获取使用人指纹的扫描图象；获取使用人视网膜图案的第二图象。

8.根据权利要求2的方法，其特征在于获取使用人物理特征图象的步骤包括以下步骤：获取使用人指纹的扫描图象；获取使用人的音纹。

9.根据权利要求2的方法，其特征在于获取使用人物理特征图象的步骤包括以下步骤：获取使用人视网膜图案的扫描图象；获取使用人的音纹。

10.根据权利要求1的方法，还包括对到远程数据库和从远程数据库来的

数据通信进行加密的步骤。

11.根据权利要求 2 的方法，还包括对到远程数据库和从远程数据库来的数据通信进行加密的步骤。

12.根据权利要求 1 的方法，还包括当使用人被授权使用卡片时,从预定菜单系统中选择所需电子业务的步骤。

13.一种用于确认信用卡/标识卡授权使用人的设备,卡片包含位于其上的具有卡片所有人信息的信息条和分配给卡片所有人的标识码,设备包括:

扫描卡片信息条并从信息条获取标识码的扫描装置;

与远程数据库通信并在数据库中查找与标识码对应的信息档案的装置;

获取卡片使用人物理特征图象的装置;

比较获取的卡片使用人图象和存储在卡片所有人信息档案中的、相应的卡片所有人物理特征图象,以正确识别卡片使用人是卡片所有人,并依据使用人图象与相应的所有人图象的匹配情况,授权使用人把卡片用于所需目的的装置;和

在使用人物理特性图象与存储在卡片所有人信息档案中的、相应的卡片所有人物理特征图象不匹配的情况下,记录所获取的卡片使用人图象的装置。

14.根据权利要求 13 的设备，其特征在于获取使用人物理特征图象的装置包括指纹扫描装置,存储的所有人物理特征图象包括存储的卡片所有人指纹图象。

15. 根据权利要求 13 的设备，其特征在于获取使用人物理特征图象的装置包括获取使用人音纹的麦克风,存储的所有人物理特征图象包括存储的卡片所有人音纹。

16.根据权利要求 13 的设备，其特征在于获取使用人物理特征图象的装置包括获取使用人视网膜图案的视网膜扫描装置,存储的所有人物理特征图象包括存储的卡片所有人视网膜图案的图象。

17.根据权利要求 13 的设备，其特征在于获取使用人物理特征图象的装置包括照片扫描装置,存储的所有人物理特征图象包括存储的卡片所有人面部特征的照片图象。

18.根据权利要求 13 的设备，还包括对设备和数据库之间的数据通信进行加密和解密的加密装置,数据库包括相应的加密装置。

确认具有未授权用户物理特征记录的信用卡的使用的系统

技术领域

本发明涉及确认信用卡和/或标识卡（身份证）授权使用人的方法和设备，特别是涉及利用数个扫描测点确认卡片的授权使用人的方法和设备。

背景技术

最近，已经尝试着开发这样的系统以防止信用卡未被授权使用。典型地，这些系统利用各种设备认证卡片使用人的身份。一种系统在卡片的表面提供了卡片所有人的指纹，其中使用人的指纹必须与卡片上的指纹匹配。利用指纹标识来确认信用/标识卡真实性的概念是众知的。美国专利Nos.4，582，985（Lofberg）和5，180，901（Hiramatsu）分别公开了一种典型的系统。然而，需要把使用人的指纹和卡片所有人的指纹进行比较的指纹识别具有一些缺点，即信用卡很容易被窜改，例如，所有人的指纹被未被授权使用者的指纹代替。

其它一些识别卡片授权使用人的方法也有相同的缺点。例如，美国专利No.4，995，086（Lilley et al.）公开了一种确认系统，其中具有卡片所有人信息的条形码位于卡片上并与保存在与系统通讯的数据库中的信息进行比较。与指纹识别类似，卡片表面上的条形码可能被窜改。

发明内容

现在，需要有一种确认信用/标识卡授权使用人的方法和设备，可以检测卡片是否被修改以便防止未被授权使用人使用卡片。

在本发明的几个目的当中提供了一种用于确认信用/标识卡授权使用人的改进方法，该方法能够检测到卡片是否被窜改;提供了一种具有数个交叉校对步骤的改进方法，该步骤能够基本上确保卡片的授权使用;提供了一种方法，该方法能够确认卡片使用人的指纹是否与卡片所有人的指纹匹配;提供了一种方法，该方法能够确认卡片使用人的音纹是否与卡片所有人的音纹（voice print）匹配;提供了一种方法，该方法能够确认卡片使用人的视网膜图案是否与卡片所有人的视网膜图案匹配;提供了一种方法，该方法可以扣留未被授权使用人的卡片;提供了一种方法，该方法可以记录未被授权使用人的指纹。

在本发明的几个目的当中，提供了一种确认信用/标识卡授权使用人的改进型设备;提供了一种设备，该设备可以检测到卡片是否被窜改;提供了一种设备，该设备具有数个扫描装置可以基本保证卡片的授权使用;提供了一种设备，该设备具有指纹扫描装置和辅助装置，用于确认卡片使用人的指纹是否和卡片所有人的指纹匹配;提供了一种设备，该设备具有麦克风和辅助装置，用于确认卡片使用人的音纹是否和卡片所有人的音纹匹配;提供了一种设备，该设备具有视网膜扫描装置和辅助装置，用于确认卡片使用人的视网膜图案是否和卡片所有人的视网膜图案匹配;提供了一种设备，该设备可以扣留未被授权使用人的卡片;提供了一种设备，该设备可以记录未被授权使用人的指纹;提供了一种设备，该设备在与中央数据库通讯时对数据传输进行加密。

通常，确认信用标识卡授权使用人的方法包括以下步骤:

a 插入卡片到具有数个扫描测点的设备中，卡片包括一个表面，在其上具有一个包含卡片所有人信息的条形，例如标识码（身份证号）和其它私人数据，在其上至少有一个卡片所有人的指纹;

b 在设备的信息条扫描测点，扫描卡片上的条形，以确认包含标识码的卡片信息;

c 比较储存在卡片条形中的信息和至少储存在与设备通讯的一个可访问数据库中的信息，如果卡片上的信息与存储在数据库中卡片所有人的信息不匹配，设备扣留卡片;

d 在设备的图形扫描测点，扫描卡片的表面，该测点通过对表面的每条线成象而把卡片的表面数字化;

e 把卡片表面的图象转换为数字化数字序列;

f 比较经图形扫描装置扫描之后而转换为数字化数字序列的卡片表面和存储在数据库中的数字化数据序列，以确定卡片是否被窜改，如果卡片的表面与存储在数据库中的卡片表面不匹配，设备扣留卡片;

g 获取使用人的指纹;

h 在指纹扫描测点，扫描使用人的指纹;

i 比较使用人的指纹和卡片上的指纹以及数据库中的卡片所有人的指纹，以确保卡片的授权使用，如果指纹扫描测点扫描到的指纹与卡片上的指纹以及数据库中的指纹不匹配，设备扣留卡片，由此依据使用人的指纹和卡片上的指纹以及数据库中的指纹的匹配情况可以确保卡片的使用人就是卡片的所有人，设备允许使用人把卡片用于预定目的。

实现本发明方法的设备包括信息条扫描装置，用于扫描卡片的信息条，和一种装置，该装置用于比较包含在条形内的信息和至少储存在一个与设备通讯的可访问数据库中所有人信息。如果卡片上的信息与存储在数据库中的卡片所有人信息不匹配，设备扣留卡片。设备和数据库包括加密装置，用于对设备和数据库间的数据传输进行加密。图形扫描装置扫描卡片的表面，其中图形扫描装置通过对表面的每一条线成象而把卡片表面数字化。适宜的装置把卡片表面的图象转换为数字化数字序列并比较经图形扫描装置扫描之后而由转换装置转换为数字化数字序列的卡片表面和存储在数据库中的数字化数字序列，用于判定卡片是否被修改。如果卡片表面与存储在数据库中的卡片表面不匹配，设备扣留卡片。具有台板（pad）的指纹扫描装置扫描使用人的指纹，卡片使用人用手指压在台板上以获取使用人的指纹，相应的装置比较使用人的指纹和卡片上的指纹以及数据库中的指纹以确保卡片的授权使用。如果指纹扫描装置扫描到指纹与数据库中的指纹以及卡片上的指纹不匹配，设备扣留卡片。这样，依据使用人的指纹与卡片上的和数据库中指纹的匹配情况可以确保卡片的使用人是卡片的所有人，设备允许使用人把卡片用于特定目的。

本发明的其它目的、特点和优点将随着描述的进行而变得明显，当与附图一起考虑时。

附图说明

在附图中示例了实现本发明的最佳模式:

图一示例了本发明的确认信用和/或标识卡授权使用者方法的流程图;

图二是实现本发明方法的设备框图;

图三是本发明的信用卡;

图四示例了示于图三的信用卡背面。

相同的参考号在几个附图当中表示相同的部分。

具体实施方式

现参照附图由 10 指示的方法(示于图 1)用于确认由 12 指示的信用和/或标识卡(示于图 3)授权使用人。优选地，卡片 12 包括一个表面 14，该表面至少具有一个印在其上的卡片 12 所有人的指纹 18。卡片优选的具有一个背面 15(图 4)，该背面具有一个印在其上的包含卡片所有人信息，例如标识码和其它私人数据，的信息条 16，例如条形码或磁条。信息条 16 和指纹

18 可以直接印到卡片 12 上并利用任何在本领域中周知的、适宜的压膜技术保护起来。如图三所示，卡片 12 具有两个印在表面 14 上的卡片所有人指纹 18。卡片 12 还可以包括其它信息，例如所有人的照片 20 以及所有人的姓名和住址。应当理解的是本发明的方法 10 适用于任何需要确认或认证卡片 12 使用人是卡片所有人的场合。本发明的方法特别适用于确认信用卡使用人。方法 10 还可以用于确认想进入受限区域(例如医院、合作研究部门等)的授权人身份。图 2 示例了由 22 指示的实现本发明方法的设备，设备 22 将在描述本发明方法 10 之后详细描述。

现参照图 1，方法 10 包括以下步骤:插入卡片 12 到设备中，例如设备 22，该设备具有数个扫描测点，即信息条扫描测点 30，图形扫描测点 32，指纹扫描测点 34，音纹记录测点 36，视网膜扫描测点 38，和照片扫描测点 40。如在下面详述的，设备 22 可以体现为任意种设计，只要能够实现方法 10 的各个确认步骤。

在插入到设备 22 之后，卡片 12 进入用于扫描卡片 12 上的条形 16 的息条扫描测点 30，以确认包含识别码的卡片 12 的信息。该信息被传送到微处理器 42(图 2)，该微处理器比较储存在信息条 16 上的、包括卡片所有人识别码的信息，和至少储存在一个与设备 22 的微处理器 42 通讯的可访问数据库 44(图 2)中所有人的信息。为了确保设备和数据库间数据传输绝对安全，设备和数据库优选地都包括对数据传输进行加密和解密的加密设备。如果卡片 12 的条形 16 上的信息对于特定的卡片与储存在数据库 44 中的信息匹配，卡片 12 由下一个测点检测(即图形扫描测点 32)。否则，如果卡片上的信息与储存在 44 数据库中的卡片所有人信息不匹配，设备 22 扣留卡片 12。如果被没收，卡片 12 可以被存放在设备 22 的任何适宜部分，直到设备得到维护，其中代表未被授权使用人的、且被设备 22 没收的卡片 12 可以被找到。

然后，卡片 12 又由图形扫描测点 32 检测，其中卡片 12 的表面 14 通过对表面的每一条线成象而被数字化，检查卡片 12 的表面 14 的目的是判定它是否已经被修改。卡片 12 的表面 14 的图象被转换成数字化数字序列，该序列被传送到微处理器 42，微处理器比较代表卡片表面的数字化数字序列和储存在前述数据库 44 中或者存储在与设备 22 的微处理器 42 通信的另一个可访问数据库中的卡片先验扫描信息。如果卡片 12 的数字化数字序列对于特定卡片，与存储在数据库中的数字化数字序列匹配，卡片 12 由下一

测点检测。然而，如果卡片的数字化数字序列与存储在数据库 44 中的数字化数字序列不匹配，设备扣留卡片 12 。与信息扫描测点 30 类似，卡片 12 可以被储存在设备 22 的任何适宜部分，直到设备得到维护，其中代表未被授权使用人的、且被设备没收的卡片可以被找到。

如图一所示，卡片 12 接下来由指纹扫描测点 34 检测。本发明方法 10 的这一步骤要求卡片 12 的使用人提供指纹 18，该指纹用来与卡片 12 上的指纹 18 以及前述数据库 44 或者与设备 22 的微处理器 42 通信的独立访问数据库中卡片所有人的指纹进行比较，以确保卡片 12 的授权使用。与信息条和图形扫描测点 30 、 32 类似，如果指纹扫描测点扫描到的指纹与卡片上的指纹或数据库 44 中的指纹不匹配，设备 22 扣留卡片 12 。如果使用人的指纹与卡片 12 上的指纹以及数据库 44 中的指纹匹配，设备 22 将允许使用人把卡片 12 用于特定目的，或者如图一所示，如果需要更加严密的确认级别，卡片 12 可以由后续测点检测。

当使用人与卡片 12 上的指纹 18 或者存储在数据库 44 中的卡片所有人指纹不匹配时，本发明方法还包括记录使用人指纹的步骤。该附加步骤的目的是为了获得线索，该线索可用于识别卡片的未被授权使用人。被记录的未被授权使用人指纹可以与存储在其它数据库中的指纹进行比较，例如罪犯档案数据库、雇员数据库等。

如上所述，如果需要附加确认，卡片 12 可以由音纹记录测点 36 、视网膜扫描测点 38 和照片扫描测点 40 检测。应当理解的是这些附加扫描步骤中的任何一个都可以独立地或者以任何组合方式执行，仍属于本发明的范围。

仍参照图一，本发明的方法 10 要求卡片 12 的使用人对设备 22 的音纹记录测点 36 讲话，以获取得使用人的音纹。该音纹被数字化后传送给微处理器 42 ，在那里该音纹与储存在数据库 44 或者储存在与微处理器 42 通讯的独立访问数据库中卡片 12 所有人的音纹进行比较。与其它测点相似，如果使用人的音纹与存储在数据库 44 中所有人的音纹不匹配 设备 22 扣留卡片 12 直到得到正确的处理。否则，设备 22 允许使用人把卡片 12 用于特定目的，或者如果需要更加精确的确认级别，卡片 12 可以由后续测点检测。

相应地，方法 10 还要求卡片 12 的使用人观察设备 22 的视网膜扫描测点 38 ，以获取使用人的视网膜图案。然后该视网膜图案被传送到微处理器 42 ，并与储存在数据库 44 或者储存在与微处理器 42 通讯的独立访问数据

库中卡片所有人的视网膜图案进行比较。与其它测点类似，如果使用人的视网膜图案与存储在数据库 44 中的所有人视网膜图案不匹配，设备 22 没收卡片。如果使用人的视网膜图案与储存在数据库 44 中的所有人的视网膜图案匹配，设备 22 允许使用人把卡片 12 用于特定目的，或者卡片 12 由后续的照片扫描测点 40 检测。

在照片扫描测点 40，卡片 12 上的照片 20 被扫描并与储存在数据库 44 中的卡片所有人的照片进行比较，以确保卡片 12 没有被窜改。该扫描测点 40 优选地比图形扫描测点 32 灵敏，因为后者用来定位卡片 12 的各个部分而不是所有人照片的细节．这样，如果卡片 12 的所有人照片 20 被使用人的照片代替，并且卡片通过图形扫描测点 32 而没有被没收，微处理器 42 将识别出照片并不匹配，由此设备 22 没收卡片 12 ．如果照片匹配，设备将允许使用人把卡片用于预定目的，确认程序结束。

现转到图二，示例了本发明的设备 22，该设备包括信息扫描装置 50，图形扫描装置 52，指纹扫描装置 54，数字化声音的麦克风 56 和装置 58，视网膜扫描装置 60 和照片扫描装置 62．微处理器 42 获取这些装置搜集到的信息，并把它们与存储在数据库 44 中的信息，或者如前所述，与存储在数个与微处理器 42 通信的独立数据库中的信息进行比较。设备 22 和数据库 44 优选地包括对其间的数据传输进行加密和解密的加密设备 63 ．加密设备 63 在确认过程中有效地阻止其他人接入电话线以非法盗取或拷贝数据传输．所考虑的加密设备 63 由 Datotek， Inc.of Dallas， TX 制造。设备 22 可以包含各种形式，然而可以预见的是它的构造方式类似于自动取款机 (ATM)，或者是用于接受和处理卡片的类似装置。

更加明确地讲，信息条扫描装置 50 用于扫描卡片 12 的条形码或磁条。如图所示，微处理器 42 包括装置 44，该装置比较包含在卡片 12 的条形 16 中的信息(包括卡片所有人的标识码)和储存在数据库 44 中所有人信息。如果卡片 12 上的信息与数据库 44 的信息不匹配，设备 22 没收卡片 12 。信息条扫描装置 50 可以是任何一种商业上可以得到的条型码扫描仪，例如 Symbol Technologies， Inc.， Bohemia， NY 出售的型号为 PDF417 的扫描仪．

图形扫描装置 52 扫描卡片 12 的表面 14，以判定卡片 12 是否被更改。转换器 66(广义的讲，转换装置)用于把卡片 12 的表面 14 的图象转换为数字化数字序列。该数字化数字序列被传送到还包括装置 68 的微处理器 42，

该装置用于比较经图形扫描装置 52 扫描后由转换器 66 转换为数字化数字序列的卡片 12 的表面 14 和存储在数据库 44(或其它与微处理器通讯的数据库)中的数字化数字序列，以判定卡片 12 是否被窜改。如果表示卡片 12 的表面 14 的数字化数字序列与数据库 44 中的数字化数字序列不匹配，设备 22 扣留卡片 12。图形扫描装置 52 和转换器 66 可以是任何一种商业上可以得到的图形扫描议和转换器，例如 Hewlett-Packard Corporation of California 制造的扫描仪。

指纹扫描装置 54 具有一个台板(未示出)，卡片 12 的使用人把手指压在其上以获取使用人的指纹。指纹扫描装置 54 扫描由台板得到的使用人指纹，并把它传送给包括装置 70 的微处理器 42，该装置用于比较使用人的指纹和卡片 12 上的指纹以及数据库 44 中的卡片所有人的指纹。如果卡片使用人的指纹 18 与卡片 12 上的指纹 18 或者与数据库 44 中的指纹不匹配，设备 22 扣留卡片。

指纹扫描装置 54 还可以包括一个记录装置(未示出)，在其中记录未被授权使用人的指纹以备后用，例如把它与其它数据库的指纹进行比较。该记录装置将有助于抓获未被授权的使用人。

指纹扫描装置 54 可以是任何一种商业上可以得到的指纹扫描系统，例如 Electronic Data Systems Corp.， Dallas， TX 出售的指纹扫描仪或者 Lofberg and Hiramatsu 专利公开的指纹扫描仪。

至此所述的设备 22 能够完成本发明的方法 10， 即，能够比较卡片 12 的条形 16 上的信息和数据库中的所有人信息，判定卡片 12 是否被修改，并比较使用人的指纹和卡片 12 上的指纹 18 以及数据库 44 中的指纹。设备 22 还包括前述的、用于记录使用人声音的麦克风 56 和辅助装置 58，以及视网膜扫描装置 60 和照片扫描装置 62，用于提高确认级别。应当理解的是根据所需的确认级别，设备 22 可以包括每个附加设备或者它们的任意组合。

麦克风 56 用于在使用人讲话时接收使用人的声音. 录音机 58(广义地讲，录音装置)在使用人对着麦克风 56 讲话之后，记录使用人的声音并把模拟信号转换为数字信号以获取使用人的音纹。音纹被传送到包括装置 72 的微处理器 42，该装置比较使用人的音纹和储存在数据库 44 或其它可访问数据库中的卡片所有人的音纹。如果卡片 12 使用人的音纹与数据库 44 中的音纹不匹配，设备 22 没收卡片 12. 麦克风 56、录音机 58 和声音识

别软件可以包括任何商业上可以得到的声音识别系统，例如 Texas Instruments of Dallas， TX 出售的声音识别系统。

视网膜扫描装置 60 在使用人观察视网膜扫描装置 60 之后获取使用人的视网膜图案。视网膜图案被传送到包括装置 74 的微处理器 42，该装置比较使用人的视网膜图案和储存在数据库 44 或者其它可访问数据库中卡片 12 所有人的视网膜图案。如果卡片 12 使用人的视网膜图案与数据库 44 中的视网膜图案不匹配，设备 22 扣留卡片 12。视网膜扫描装置 60 可以从 Ophthalmic Imaging Systems， Inc. of Sacramento， CA 购买。

最后，设备 22 包括照片扫描装置 62，该装置用于扫描卡片 12 上的照片 20。该扫描装置 62 优选地比图形扫描装置 54 灵敏，因为后者用于定位卡片的主要部分而不是卡片所有人的照片细节。该信息被传送到包括装置 76 的微处理器 42，该装置比较扫描装置 62 扫描到的照片 20 和储存在数据库 44 或者其它可访问数据库中的卡片 12 的所有人的照片，以确保卡片 12 没有被窜改，即照片 20 没有被使用人的照片所代替。如果卡片 12 上的照片 20 与数据库 44 中的照片不匹配，设备 22 扣留卡片。照片扫描装置 62 可以从 Hewlett-Packard Corporation 购买。

设备 22 的微处理器 42 可以从商业上可以得到的微处理器中选择，其中软件包括一个菜单系统，例如 Galacticomm， Inc. of Ft. Lauderdale， FL 设计的系统。可以预见的是当卡片的授权使用人被确认时，该菜单系统使卡片的使用人能够从多个选项中选择，例如信用、存款、现金传送、医院或健康护理授权等。在该连接中，软件可以设计为单一用途。例如，医院在接纳或治疗前需要健康护理授权。系统软件可以专门设计为访问和存储适宜的帐单数据，例如日期、治疗类型、设施的位置等。其它单用途应用，例如银行的 ATM，将访问和存储与各自目的有关的信息。还应考虑的是设备代码和位置应当编码为条形码的形式，并贴在设备内部，其中独立条形码阅读机(未示出)将读取条形码并用关于每次卡片业务的信息存储信息。

应当注意的是本发明的方法 10 和设备 22 能够确认信用/标识卡的授权使用人，或者能够判定卡片是否被修改。

这里显示并描述了特定的、体现本发明的具体结构，对于本领域的技术人员很明显的是在不偏离基本发明概念的宗旨和范围的前提下可以对各个部分进行修改和重配置，本发明并不受限于除附属权利要求范围之外的、在这里显示并描述的形式。

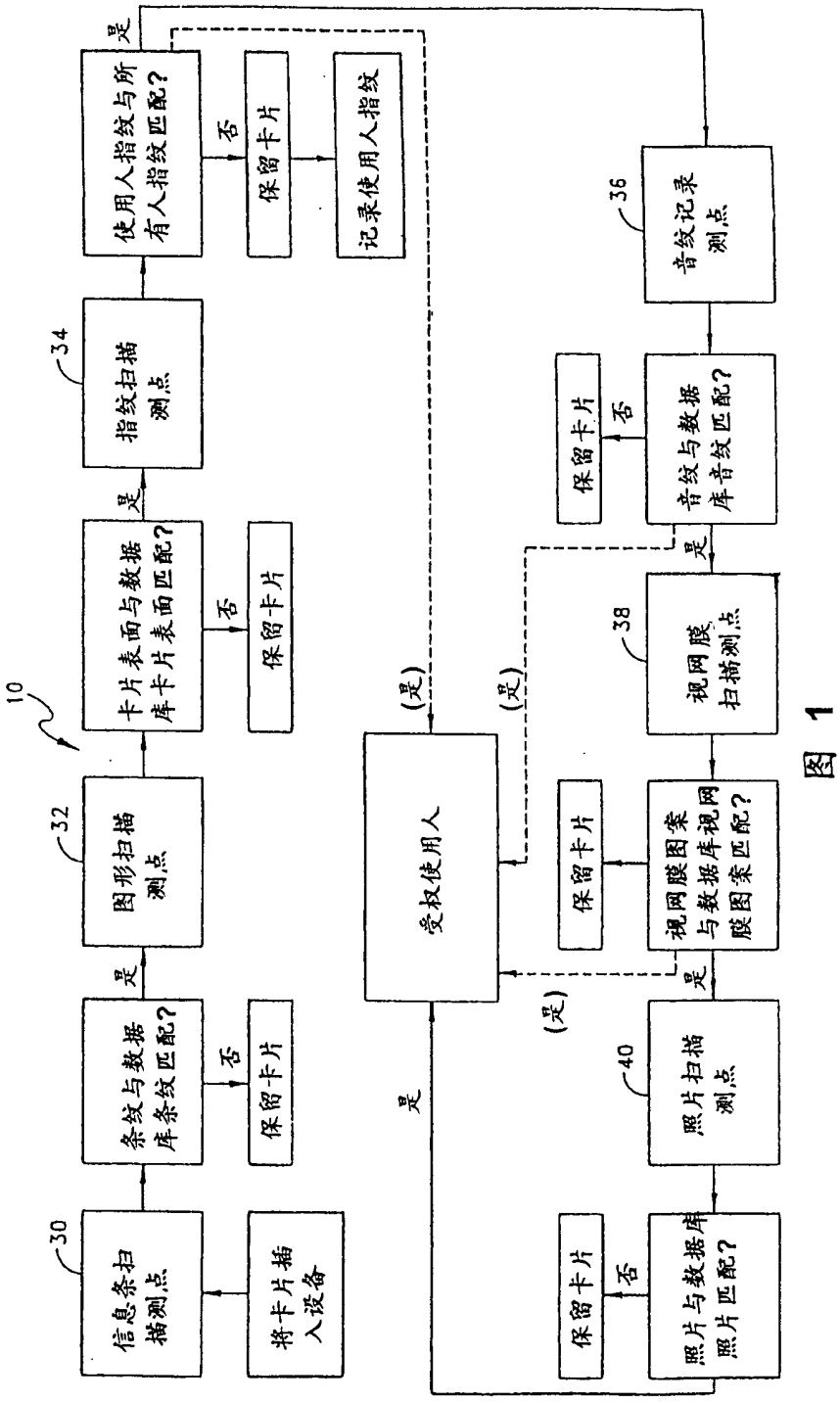

10
30
信息条扫描测点
将卡片插入设备
条纹与数据库条纹匹配?
是
否
保留卡片
32
图形扫描测点
卡片表面与数据库卡片表面匹配?
是
否
保留卡片
34
指纹扫描测点
使用人指纹与所有人指纹匹配?
是
否
保留卡片
记录使用人指纹
受权使用人
是
(是)
(是)
(是)
是
保留卡片
照片与数据库照片匹配?
否
40
照片扫描测点
视网膜图案与数据库视网膜图案匹配?
是
否
保留卡片
38
视网膜扫描测点
音纹与数据库音纹匹配?
是
否
保留卡片
36
音纹记录测点

图 1

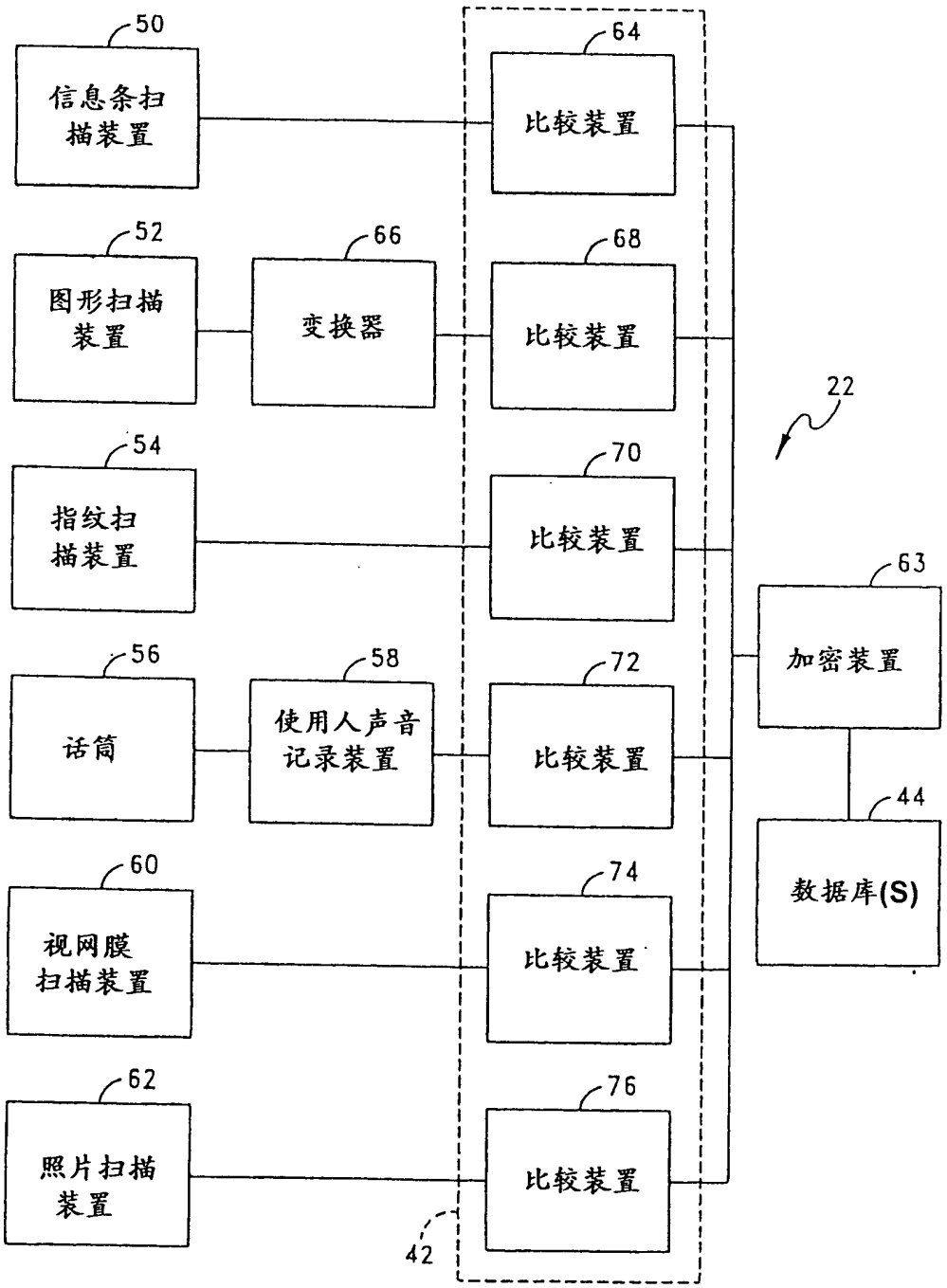

50
信息条扫描装置
52
图形扫描装置
54
指纹扫描装置
56
话筒
58
使用人声音记录装置
60
视网膜扫描装置
62
照片扫描装置
66
变换器
64
比较装置
68
比较装置
70
比较装置
72
比较装置
74
比较装置
76
比较装置
42
22
63
加密装置
44
数据库(S)

图 2

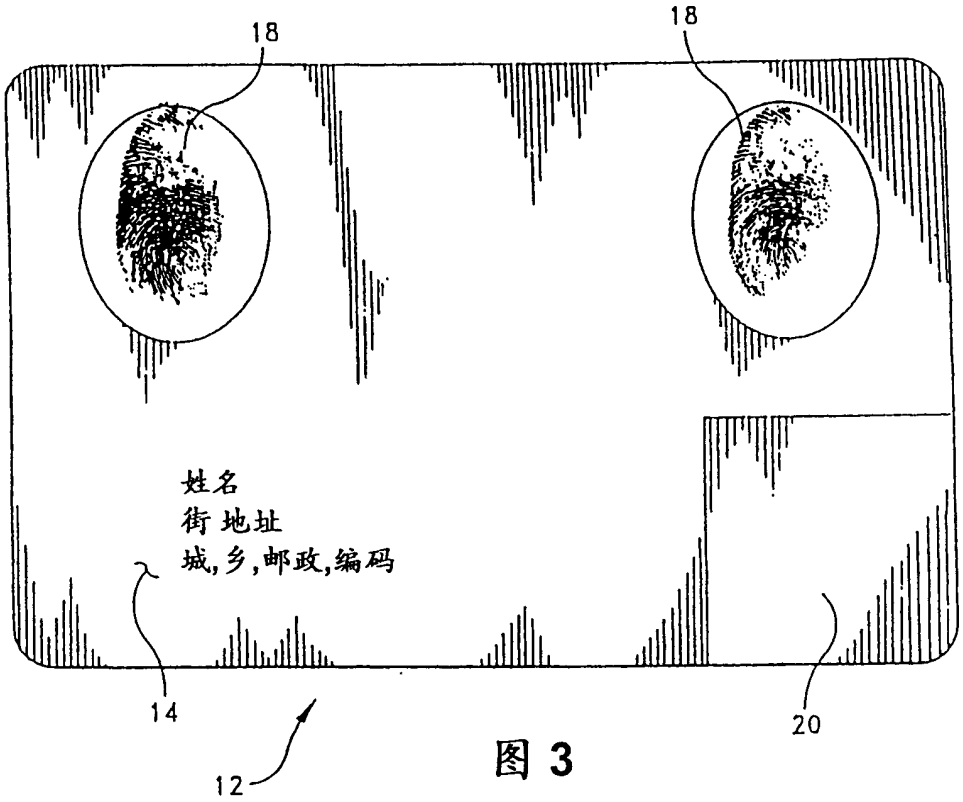


图 3

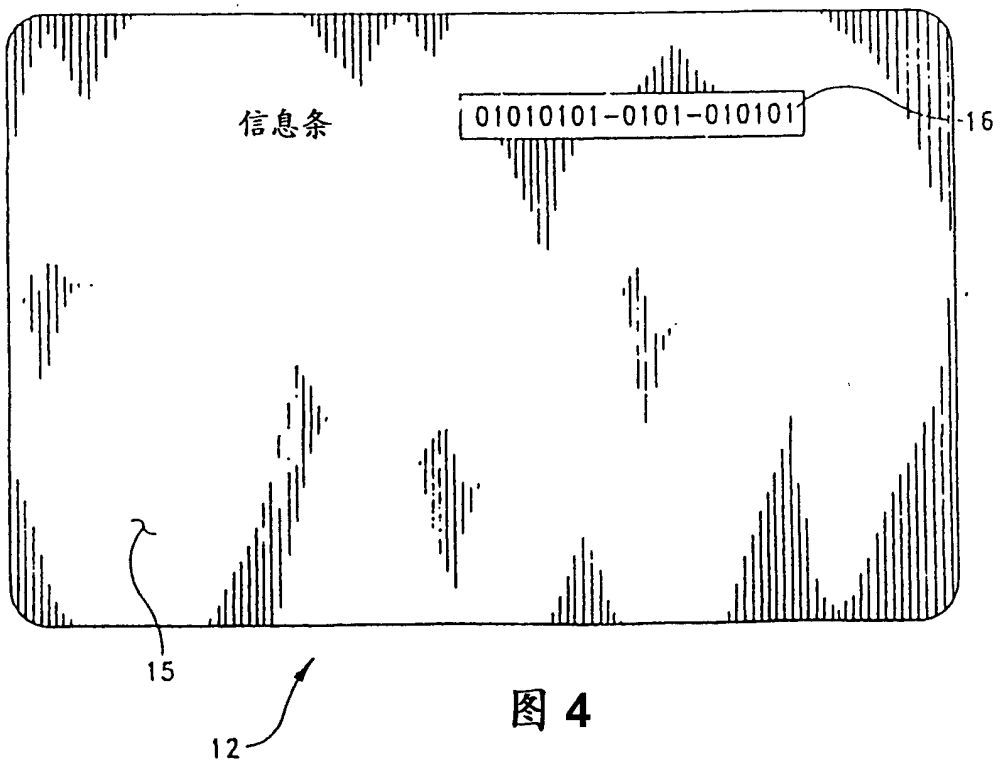


图 4