

一种指纹识别无线射频卡的身份认证系统及方法

申请号：[200510086958.8](#)

申请日：2005-11-23

申请(专利权)人 [中国科学院自动化研究所](#)
地址 [100080北京市海淀区中关村东路95号](#)
发明(设计)人 [田捷](#) [谢卫华](#) [时鹏](#) [杨鑫](#)
主分类号 [G06K9/00\(2006.01\)I](#)
分类号 [G06K9/00\(2006.01\)I](#) [G06K7/00\(2006.01\)I](#)
公开(公告)号 [1971581](#)
公开(公告)日 [2007-05-30](#)
专利代理机构 [中科专利商标代理有限责任公司](#)
代理人 [段成云](#)

[19] 中华人民共和国国家知识产权局

[51] Int. Cl.

G06K 9/00 (2006.01)

G06K 7/00 (2006.01)



[12] 发明专利说明书

专利号 ZL 200510086958.8

[45] 授权公告日 2009年2月4日

[11] 授权公告号 CN 100458829C

[22] 申请日 2005.11.23

[21] 申请号 200510086958.8

[73] 专利权人 中国科学院自动化研究所

地址 100080 北京市海淀区中关村东路 95 号

[72] 发明人 田捷 谢卫华 时鹏 杨鑫

[56] 参考文献

CN2416548Y 2001.1.24

CN2480914Y 2002.3.6

基于纹线跟踪的指纹细节提取算法. 杨小冬, 宁新宝, 谭台哲. 计算机应用, 第 24 卷第 3 期. 2004

审查员 李紫峰

[74] 专利代理机构 中科专利商标代理有限责任公司

代理人 段成云

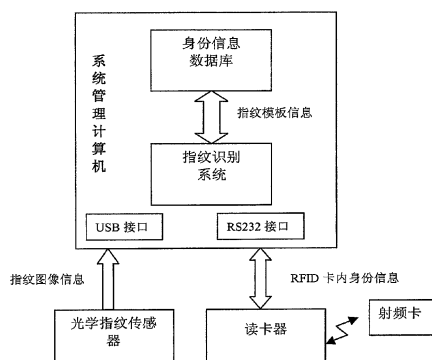
权利要求书 3 页 说明书 7 页 附图 4 页

[54] 发明名称

一种指纹识别无线射频卡的身份认证系统及方法

[57] 摘要

本发明涉及图像识别技术领域,特别是一种采用指纹识别技术和无线射频卡的身份认证系统及方法。系统包括:计算机、无线射频卡、读卡器、光学指纹传感器。方法包括:(1)用户信息的管理;(2)个人指纹信息的管理;(3)读出存储在无线射频卡上的信息;(4)个人身份认证在计算机主机内进行。由于指纹特征的唯一性,本发明可以有效的防止由于卡被盗用而引起的无线射频卡管理系统的安全隐患。由于本发明关键性的指纹库的建立和比对过程均在服务器上完成,无需在已发放卡中增加额外信息,便于系统升级和管理,有明显的经济效益。



1. 一种基于无线射频卡的指纹身份识别系统，其特征在于，包括：
 - 一台用于实现指纹数据采集，无线射频卡信息处理，身份认证的计算机，该计算机至少有一个标准的 USB 接口，以及串行接口，所述计算机还具有储存和分配给用户 ID 号及指纹相关信息的数据库，其中每一条指纹信息和一个 ID 号唯一绑定；
 - 一个无线射频卡，该卡里存有基本的个人信息，以及一个唯一的标识的 ID 号，用于在计算机读取后检索身份数据库；
 - 一台用于连接该计算机的指纹传感器，该传感器是适合于大规模指纹认证系统使用的光学指纹传感器，并有 USB 接口和上述的计算机相连，用于采集用户的指纹信息，将所采集的指纹信息传送给所述计算机，在所述计算机内具有指纹模板，计算机基于比对特性有效性权值，比对用的指纹信息以数据库的形式保存，判断指纹图像各个细节节点的可靠性，动态更新相应的指纹模板，从而动态更新数据库，实现个人身份的鉴别；
 - 一台使用上述无线射频卡的读卡器，该读卡器使用串行接口和计算机相连，用于读取无线射频卡的信息。
2. 根据权利要求 1 中所述的系统，其特征在于：所述计算机在登陆系统时要求采集个人的指纹信息进行使用者身份的确认，并独立采集指纹信息并执行指纹识别方法进行身份的确认，计算机的通讯接口采用 USB 接口用于和光学指纹传感器相连，串行接口用于和非接触式读卡器相连。
3. 根据权利要求 1 中所述的系统，其特征在于：非接触的无线射频卡中存储的个人身份信息是加密的。
4. 根据权利要求 1 中所述的系统，其特征在于：所述无线射频卡的读卡器是和该无线射频卡配套使用的专用的读卡器，且与计算机正常通讯。
5. 根据权利要求 1 中所述的系统，其特征在于：所述指纹传感器是光学指纹传感器。
6. 一种基于无线射频卡的指纹身份认证方法，这种方法包括如下步骤：

(1) 用户信息的管理功能, 将基本的用户信息写入无线射频卡的相关区域中;

(2) 个人指纹信息的管理功能, 建立与个人用户相关的数据库, 并采集用户的指纹信息, 与其它标识个人身份的相关信息一起存入计算机的数据库中, 用于身份认证的指纹比对; 一个用户存储四个指纹模板用于身份认证, 指纹模板在使用中动态更新;

(3) 读出存储在无线射频卡上的信息;

(4) 个人身份认证在计算机主机内进行, 对于每个指纹模板的使用情况进行统计分析并给出细节点集的使用情况分析报告, 同时给出指纹模板的有效性的分数报告和细节点有效性分数报告, 把指纹传感器传送的指纹图像信息与数据库中的储存指纹特征模板信息应用指纹识别方式进行比对认证; 并且如果比对成功, 则给持卡用户相应的授权。

7. 根据权利要求6所述的方法, 还包括以下步骤:

如果读出的指纹信息与储存的持卡人指纹信息不匹配, 则向持卡用户显示拒绝登陆信息。

8. 根据权利要求6所述的方法, 其特征在于: 用于身份认证的计算机的管理者采用指纹识别的方式登陆。

9. 根据权利要求6所述的方法, 其特征在于: 指纹身份识别是比对射频卡指示的用户。

10. 一种指纹自动识别方法, 该方法为基于无线射频卡管理系统的专用指纹识别方法, 用于对持卡人指纹信息的快速识别, 判定持卡人的身份, 包括如下步骤:

(1) 对采集的指纹图像经过增强处理并提取指纹细节点 $M = \{M_k, 1 \leq k \leq L\}$, 对于其中任意一个细节点, 由其特征矢量为 $M_k = (x_k \ y_k \ \varphi_k \ t_k)^T$ 构成指纹的基本模板, 基于比对特性有效性权值的办法对指纹模板比对, 构成一个比对特性有效性权值的数组, 分析各次比对特性权值的分布情况, 判断出各个细节点的可靠性, 从而动态更新相应的指纹模板;

(2) 求指纹方向场, 是分析四个指纹图像中灰度点的梯度方向 0° 、 45° 、 90° 和 135° 和待估计方向的关系, 利用模糊逻辑的方法去求解指

纹图像四个方向所对应的方向值所占比例为 $[\partial_1, \partial_2, \partial_3, \partial_4]$;

若映射 $[0^\circ - 180^\circ]$ 为 $[0-128]$ 中的值, 从而估计出所求的方向场为:

$O = \partial_1 + \partial_2 \times 32 + \partial_3 \times 64 + \partial_4 \times 96$, 其中 1、32、64 和 96 分别对应四个方向 0° 、 45° 、 90° 和 135° 所对应的方向值;

(3) 利用一个基于具有方向性的平行四边形的模板和滑动窗对方向场进行滤波, 获得增强的指纹图像;

(4) 对增强的指纹图像通过跨越脊线的断面进行线积分, 对于脊线方向在 $[\frac{\pi}{4} \frac{3\pi}{4}]$ 之间的线积分采用垂直于 y 轴方向的变换, 对于脊线方向在 $[0 \frac{\pi}{4}]$ 和 $[\frac{3\pi}{4} \pi]$ 之间的情况采用垂直于 x 轴方向的变换, 得到细化图像, 完成指纹比对功能, 通过比对的结果给出“是”或“否”来完成对个人身份的识别。

一种指纹识别无线射频卡的身份认证系统及方法

技术领域

本发明涉及图像识别技术领域，特别是一种采用指纹识别技术和无线射频卡的身份认证系统及方法。

背景技术

无线射频卡是一种应用比较广泛的标识使用者身份的 ID 卡，这种 ID 卡的使用十分方便，只要用户使用无线射频卡来划过无线射频卡的读卡器即可。读卡器读出卡内储存的信息，并将信息传送到管理计算机，在计算机内完成信息处理，并对该卡所标识的 ID 做相应的操作。这种无线射频卡的系统广泛应用于在大规模的替代现金交易的场合，如校园的饭卡系统，公交车的刷卡系统等等。这种无线射频卡的基本功能是利用卡作为身份认证的手段，从而执行相应的身份认证后的应用功能。

无线射频卡在使用中存在明显的安全隐患，主要是这种射频卡不是和使用者紧密相连的，单一的由无线射频卡标识注册用户身份的方法并不能充分地防止他人对卡的盗用，时常会因为发生因他人冒用而造成卡拥有者经济上的损失。而随着当前无线射频卡的应用范围不断扩大，涉及的使用人群也越来越广，例如重要部门的门禁系统，大型机构的身份管理系统等，其安全隐患也越来越突出。

因此，非常有必要利用一种有效的方法来提高射频卡在身份认证上的能力，从而大大提高系统运行的安全性。利用指纹识别技术，将使系统不仅依靠射频卡来标识身份，而且必须提供正确的指纹才能够获得相应的权限。由于人的指纹有着唯一性和不变形的特点，因此可以将伪造或盗用无线射频卡的行为拒之门外，有效地维护系统的安全。同时，针对于无线射频卡系统的指纹身份认证技术，能够通过对于现有系统的较小改造实现系统升级，无需更换新的认证系统，可以节省相当的改造费用。因此，使用可靠性高、使用简便、对现有系统改造小的指纹认证的手段

是一个很好的解决方案。

发明内容

本发明的目的就是提供了一套指纹识别无线射频卡身份认证系统，利用高性能的指纹识别方法来进行生物特征的比对，进一步对无线射频卡的使用者进行身份的鉴别，从而保证了用户使用射频卡进行消费或其他相关活动的安全性，有效地防止了由于其他人冒用带来的损失。

本发明把指纹独一无二的特征信息用作身份认证系统中对持卡人身份的认证。持卡人在登陆身份认证系统时，首先用标识自己身份的无线射频卡通过读卡器进入识别系统，然后在光学指纹传感器上按压指纹，系统将采集到的指纹与数据库中持卡人的指纹信息进行特征比对，迅速判别出持卡人身份的真伪。由于指纹特征的唯一性，该发明可以有效的防止由于卡被盗用而引起的无线射频卡管理系统的安全隐患。并且由于该发明关键性的指纹库的建立和比对过程均在服务器上完成，无需在已发放卡中增加额外信息，便于系统升级和管理，大大提高了现有无线射频卡管理系统的安全性和科技含量，同时对现有系统的改造很小，有明显的经济和社会效益。

本发明的无线射频卡的指纹身份识别系统，包括如下几个部分：

一台用于实现指纹数据采集，无线射频卡信息处理，身份认证的计算机，该计算机至少有一个标准的 USB 接口，以及串行接口，所述计算机还具有储存和分配给所述用户 ID 号及指纹相关信息的数据库；

一个无线射频卡，该卡里存有基本的个人信息，以及一个唯一的可以标识的 ID 号；

一台用于连接该计算机的指纹传感器，该传感器是适合于大规模指纹认证系统使用的光学传感器，并有 USB 接口可以和上述的计算机相连，用于采集用户的指纹信息，将采集的指纹信息传送给所述计算机，在所述计算机内实现个人身份的鉴别；

一台使用上述无线射频卡的读卡器，该读卡器使用串行接口和主机相连，用于读取无线射频卡的信息。

所述非接触的无线智能卡中存储的个人身份信息是加密的。

一种基于无线射频卡的指纹身份认证方法，这种方法包括如下步骤：

(1) 用户信息的管理功能，将基本的用户信息写入无线射频卡的相关区域中；

(2) 个人指纹信息的管理功能，建立与个人用户相关的数据库，并采集用户的指纹信息，与其它标识个人身份的相关信息一起存入数据库中，用于身份认证的比对使用；

(3) 读出存储在无线射频卡上的信息；

(4) 个人身份认证在计算机主机内进行，把指纹传感器传送的指纹图像信息与数据库中储存的指纹特征模板信息应用指纹识别方法进行比对认证；并且如果比对成功，则给持卡用户相应的授权。

如果读出的指纹信息与储存的持卡人指纹信息不匹配，则向持卡用户显示拒绝登陆信息。

用于身份认证的计算机的管理者采用指纹识别的方式登陆。

指纹身份识别只是比对射频卡指示的用户而不是进行多用户的搜索。

一种指纹自动识别方法，该方法为基于无线射频卡管理系统的专用指纹识别方法，用于对持卡人指纹信息的快速识别，准确判定持卡人的身份，所作的改进包括如下步骤：

(1) 基于比对特性有效性权值的办法，动态进行指纹模板更新，以提高指纹模板的准确性；

(2) 求指纹方向场过程中，分析四个指纹中灰度点的梯度方向 0° 、 45° 、 90° 和 135° 和待估计方向的关系，利用模糊逻辑的方法去求解四个方向；

(3) 利用一个基于具有方向性的平行四边形的模板来进行方向滤波；

(4) 通过跨越极限的断面进行线积分，可以得到更好的细化图像，更准确地完成随后的指纹比对功能。

附图说明

图 1 是通过指纹传感器采集指纹用来提取个人身份识别过程图。

图 2 是无线射频卡的使用示意图。

图 3 是无线射频卡的基本结构示意图。

图 4 是 4 枚指纹模板用于指纹身份的模板图。

图 5 是指纹识别过程示意图。

图 6 是本发明的无线射频卡指纹身份识别系统图。

具体实施方式

根据本发明的另一方面，提供一种包含无线射频卡和指纹身份认证系统的识别个人身份的方法，这种方法包括以下步骤：

用户通过指纹传感器采集指纹用来提取个人身份识别用的模板。采集后的指纹被机器指纹图像处理单元处理之后，提取其中的指纹细节点信息作为模板并存入个人信息数据库（指纹数据库）中，用作待比对信息。过程如附图 1 所示：

无线射频卡是使用者进行身份标识的一个凭证，以下附图 2 是无线射频卡的使用示意图。使用者在办理相关的手续后获得自己的无线射频卡后，操作人员将通过系统将使用者的基本信息，包括姓名，性别等写入卡中。这个无线射频卡中还存有一个唯一识别的 ID 号，这个 ID 号连同上面的信息一并作为无线射频卡中的身份信息，用在主机读取后检索数据库过程中。

个人身份数据库是这个系统进行交互的数据平台，其基本结构见附图 3，其中的个人的姓名，性别等基本信息来源于用户提供的信息，ID 号来源于用户持有的无线射频卡的 ID 号，指纹模板信息是用户个人的生物特征信息，他是使用上面的指纹模板提取程序生成的，并作为标识用户的基本特征。所有这些信息将和无线射频卡中的信息保持一致，如果发生变化系统将根据操作自动更新。

用户的个人指纹模板是用户进行指纹身份认证的关键。系统会容许用户注册最多 4 枚指纹模板用于指纹身份的认证的依据见附图 4，由于系统的认证基本上属于一对一的指纹校验，所以过多的模板会增加识别的时间，不利于系统的实时运行。系统对于这四个模板提供了可以增加、修改和删除等管理方法，同时对于每个模板的使用情况进行统计分析并给出细节点集的使用情况分析报告，同时也给出了模板的有效性的分数

报告和细节点有效性分数报告，这两个分数用于系统管理员参考模板管理使用，当分数过低时，系统将给出提示。

指纹识别方法是指纹身份认证系统中的核心内容，采集仪捕捉到的指纹图像只有通过计算机内指纹识别方法的处理，才能提取到指纹的细节点信息，进一步与数据库中模板进行比对。

本发明所采用的指纹识别方法是一套针对于无线射频卡管理系统的要求而开发的。为了加快系统运行的速度，减少身份认证的错误率，开发出一套新的方法以适应实际的需求。其中的改进包含：

系统对于这四个模板提供了可以增加、修改和删除等管理办法。为了进一步提高指纹模板的准确性，以提高指纹识别的效率和准确性，本发明采用了以下的基于比对特性有效性权值的办法，来动态进行指纹模板更新。本方法可以提高指纹模板的准确度，从而提高系统在身份认证中的正确率。

当采集的指纹图像抽取了细节点点集 $M = \{M_k, 1 \leq k \leq L\}$ 。其中 L 是该点集中细节点的个数。对于其中任意一个细节点，其特征矢量为 $M_k = (x_k \ y_k \ \varphi_k \ t_k)^T$ ，这个特征矢量就构成了指纹的基本模板。

在指纹识别过程中需要对同一枚指纹进行多次采集，由于指纹采集的时间和环境等因素的影响，这些指纹图像不会完全重合，而会发生旋转和平移，还会发生细节点信息的丢失，每次提取的细节点集也不同，每次比对结果对于每个细节点集产生不同的比对分数。对于每个细节点信息也有类似的情况，可以构成一个比对特性有效性权值的数组，通过分析各次比对特性权值的分布情况，可以判断出各个细节点的可靠性，从而动态更新相应的模板为 M_d^T 。

动态更新模板的操作会增加系统运行的负担，在一般情况下可以采用手动管理的方式。这时对于每个模板的使用情况，系统都作出了统计分析，并给出了细节点集的使用情况分析报告。同时，给出了模板 M^T 的有效性的分数报告和细节点 M_i^T 有效性分数报告，这两个分数用于系统管理员参考模板管理使用，对于分数的异常情况将会给出提示，如果处于手动管理的时候可以选择用 M_d^T 替代 M^T 。

指纹身份认证过程是对采集的指纹图像经过增强处理并提取细节点

后，再经过指纹模板的比对，通过比对的结果给出“是”或“否”来完成对个人身份的认证。这个过程是否高效准确，将极大地影响个人身份认证系统的实际应用。本发明采用如下的方法来进一步提高识别的速度和准确性，其中包含：

(1) 指纹识别过程耗时最多的指纹图像的增强部分，其中最耗时的是方向场提取部分和方向滤波部分。对于方向场提取部分，采用的是分析四个指纹中灰度点的梯度方向 0° 、 45° 、 90° 和 135° 和待估计方向的关系，利用模糊逻辑的方法去求解出四个方向： 0° 、 45° 、 90° 和 135° 所占的比例 $[\partial_1, \partial_2, \partial_3, \partial_4]$ 。若映射 $[0^\circ - 180^\circ]$ 为 $[0-128]$ 中的值，从而估计出所求的方向场如下式， $O = \partial_1 + \partial_2 \times 32 + \partial_3 \times 64 + \partial_4 \times 96$ 。其中 1、32、64 和 96 分别对应四个方向 0° 、 45° 、 90° 和 135° 所对应的方向值。该方法只使用基本算术运算，执行速度比一般的利用两个梯度方向的反正切函数快。同时，由于采用了四个梯度方向，也比上述使用两个梯度方向的方法准确，其效果见附图 5。

(2) 对于方向滤波问题，这里采用一个基于具有方向性的平行四边形的模板来进行方向滤波的方法。同时在进行滤波的同时，利用滑动窗的方法来加速方法的运行，可以进一步提高方法执行的效率，也能够得到非常理想的图像增强效果。

(3) 为了提高指纹细节点提取方法性能，使之在处理不同宽度脊线时候不受脊线边缘性的影响。并解决在处理过程中，因指纹图像二值化和细化操作分为两步实现而降低了执行的速度的问题。本方法采用基于线积分的方法，直接从增强后的指纹图像来得到细化图像，从而提高了方法的执行速度，增强了方法的鲁棒性。

(4) 线积分通过跨越脊线的断面进行，只采用垂直于 x 轴方向或垂直于 y 方向两种情况下的处理方法。对于脊线方向在 $[\frac{\pi}{4}, \frac{3\pi}{4}]$ 之间的线积分采用垂直于 y 轴方向的变换，对于脊线方向在 $[0, \frac{\pi}{4}]$ 和 $[\frac{3\pi}{4}, \pi]$ 之间的情况采用垂直于 x 轴方向的变换。

方法实现的步骤如下：

- 1) 从第一行开始，确立线积分起始点，检查已处理标志，如已经

处理则跳过，直接处理下一点；

- 2) 对于待处理点，确定其对应的所有线积分点；
- 3) 对于这些线积分点确定各个峰、谷值点，并去除可能的干扰点，以确定线积分上下界；
- 4) 按照上述线积分特征点选取方法，选择特征点，并在已处理的点作出标记。

重复上述 1) —4) 步，直至图像所有点处理完毕。

通过上述方法得到的细化图像效果较好，可以通过它提取细节点集从而可以更准确地完成随后的指纹比对功能。

本发明所采用的无线射频卡指纹身份识别系统的工作流程见附图 6，在系统正常运行之后，系统将动态显示要求划卡的提示，进行身份识别的用户使用无线射频卡划过读卡器的感应区，当无线射频卡读卡器识别出该无线射频卡之后，读取其中存有的个人身份信息，同时划卡的提示中止。系统根据其中的个人身份信息检索个人身份数据库，从而得到其中保存的个人的指纹模板信息，这些信息将会在随后的指纹身份认证中使用。这时系统自动进入指纹身份识别过程。系统将会动态显示要求用户按捺指纹的提示，用户在指纹采集议上按指纹后，系统在采集到有效的指纹图像后，停止显示按捺指纹的提示，并显示出指纹的图像。随后系统将对采集的指纹图像和刚才检索到的指纹模板进行比对，如果比对成功则显示欢迎信息，进入随后的身份认证后的处理工作，否则将显示没有成功的提示，并自动进入上述要求重新按捺指纹的过程，动态显示要求用户按捺指纹的提示，等待用户再次按捺指纹。如超过六次以上没有正确识别，则自动返回到重新划卡的进程，动态显示要求划卡的提示，等待重新划卡。

为了保证系统各种处理功能的安全性，计算机在系统启动时要求进行指纹识别无线射频卡身份认证的登陆（可以不选择此项功能），计算机的管理者在使用管理程序前也要求进行指纹识别无线射频卡身份认证的登陆，其主要过程同上面的过程相同。

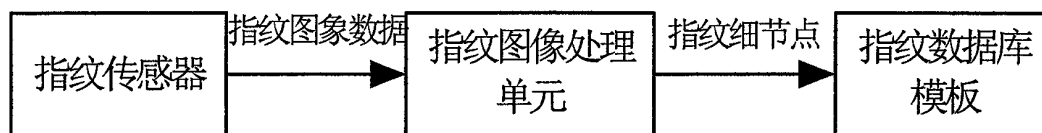


图 1

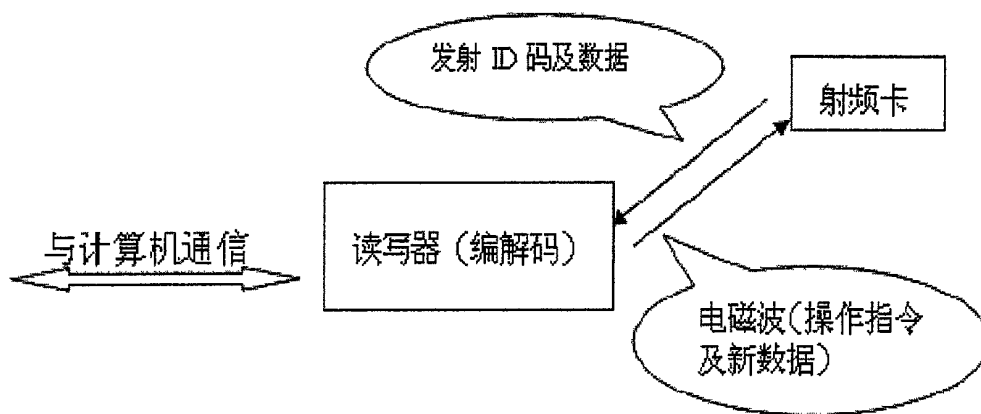


图 2

卡ID	姓名	性别	地址	公司名称	编号	指纹模板
01026ff6c3a	李明	男	北京中关村	数字ABC	01	1.MDL
01026ff6c3b	张红	女	北京中关村	数字ABC	12	1.MDL
01026ff6c3c	王亮	男	北京中关村	数字ABC	23	1.MDL
01026ff6c3d	赵广	男	北京中关村	数字ABC	34	1.MDL
01026ff6c3e	孙科	男	北京中关村	数字ABC	45	1.MDL
01026ff6c3f	钱丽	女	北京中关村	数字ABC	56	1.MDL
01026ff6c3g	周天	男	北京中关村	数字ABC	67	1.MDL
01026ff6c3h	范懿	女	北京中关村	数字ABC	78	1.MDL
01026ff6c3i	秦帆	女	北京中关村	数字ABC	89	1.MDL
01026ff6c3j	洪亮	男	北京中关村	数字ABC	910	1.MDL
01026ff6c3k	张涛	男	北京中关村	数字ABC	1011	1.MDL

图 3

指纹模板管理

增添和修改部分

模板1 模板2 模板3 模板4

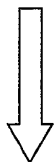
增加模板 修改模板

删除部分

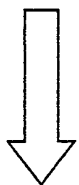
模板1 模板2 模板3 模板4

显示模板 删除模板

图 4



指纹方向场



增强特征提取及识别

图 5

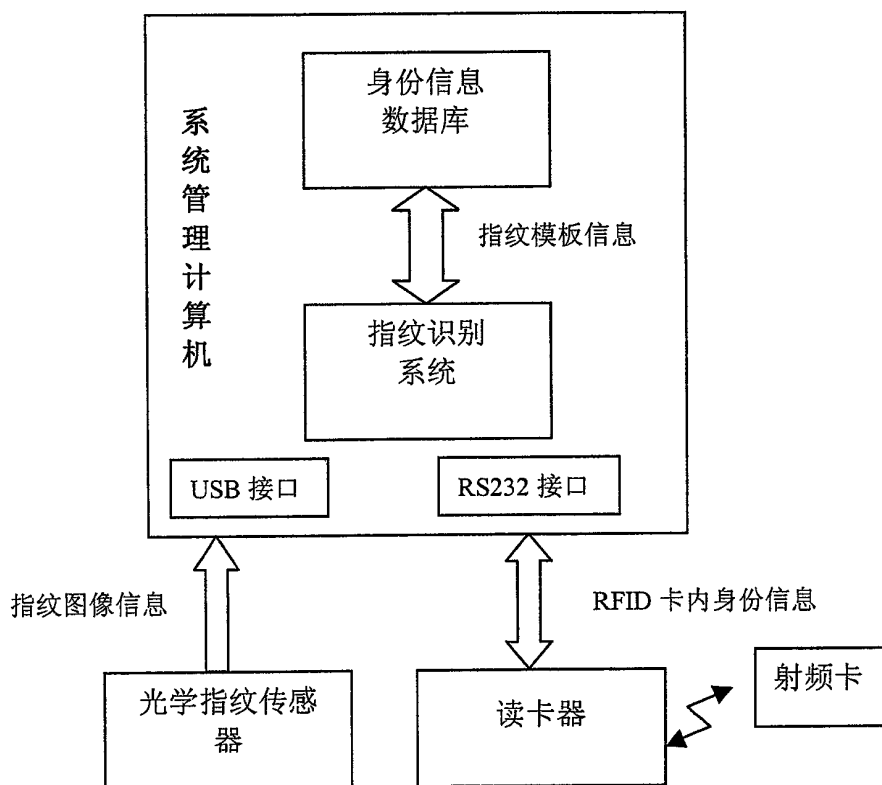


图 6