



(12) 发明专利申请

(10) 申请公布号 CN 101739742 A

(43) 申请公布日 2010. 06. 16

(21) 申请号 200910218072. 2

(22) 申请日 2009. 12. 22

(71) 申请人 中国科学院长春光学精密机械与物理研究所

地址 130033 吉林省长春市东南湖大路  
3888 号

(72) 发明人 韩秋蕾 姚志军 沈湘衡

(74) 专利代理机构 长春菁华专利商标代理事务所 22210

代理人 王淑秋

(51) Int. Cl.

G07C 9/00 (2006. 01)

G06K 9/00 (2006. 01)

G06K 9/64 (2006. 01)

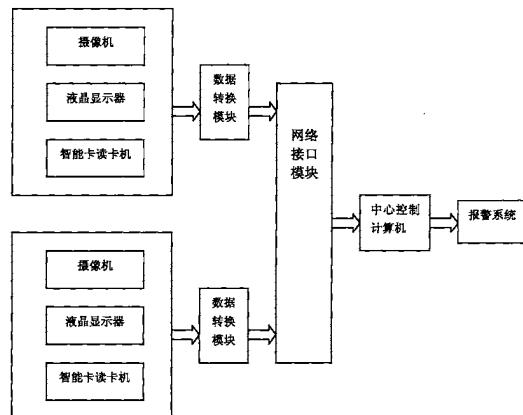
权利要求书 1 页 说明书 5 页 附图 3 页

(54) 发明名称

联网式多通道门禁考勤系统

(57) 摘要

本发明涉及一种联网式多通道门禁考勤系统，该系统的摄像机采集持卡人的人脸图像，智能读卡机采集持卡人的智能卡信息；数据转换模块将摄像机和智能读卡机采集的视频数据传输到中心控制计算机中；网络接口模块用来进行网络连接；中心控制计算机对持卡人的人脸图像和智能卡信息进行确认和分析识别，从而验证持卡人是否是智能卡的真实主人；本发明能够有效的防止冒充他人进入或代人打卡考勤的行为的发生。采用基于分块主成分分析的算法，对持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认，计算量较小，分析识别快，适用于海关监控系统，门禁系统，考勤系统等应用方向。



1. 一种联网式多通道门禁考勤系统,包括摄像机、智能卡读卡机、数据转换模块、网络接口模块、中心控制计算机;摄像机采集持卡人的人脸图像,智能读卡机采集持卡人的智能卡信息;数据转换模块将摄像机和智能读卡机采集的视频数据传输到中心控制计算机中;网络接口模块用来进行网络连接;中心控制计算机对持卡人的人脸图像和智能卡信息进行确认和分析识别,从而验证持卡人是否是智能卡的真实主人;其特征在于所述中心控制计算机的对持卡人的人脸图像和智能卡信息进行确认和分析识别的程序流程包括如下步骤:

用于系统上电以后进行自检的步骤;

用于采集持卡人的人脸图像和智能卡信息的步骤;

用于对采集来的持卡人的人脸图像进行颜色补偿的步骤;

用于利用基于肤色的人脸检测算法确定人脸的位置,进而截取出人脸图片的步骤;

用于将持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认的子程序;

所述将持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样

本图片进行比对和确认的子程序包括下述步骤:

用于建立待确认人信息数据库的步骤:

存储每个持卡人的样本图片、智能卡信息和样本图片的投影向量 $Z_{x_i}$ ;所述投影向量 $Z_{x_i}$ 按照下述方法得到的:

对存储的每个持卡人的 N 张人脸样本图片  $x_1, x_2, \dots, x_i, \dots, x_N$  进行 Census 变换去除光照影响;将变换后的每幅图像  $x_i$  分为 t 个子块,分别求得各子块的特征向量和特征值;根据设定的各子块的权重,对各子块选取不同数量的特征向量和特征值,组成每幅图像  $x_i$  的变换矩阵 $W_{x_i}$ ,并计算相应的投影向量 $Z_{x_i}$ ;

用于计算持卡人人脸图片投影向量  $Z_{var}$  的步骤:

将采集的持卡人人脸图片数据信息  $x_{var}$  进行 Census 变换去除光照影响;将变换后的图像  $x_{var}$  分为 t 个子块,分别求得各子块的特征向量和特征值;根据设定的各子块的权重,对各子块选取不同数量的特征向量和特征值,组成图像  $x_{var}$  的变换矩阵 $W_{x_{var}}$ ,最后求得  $x_{var}$  的投影向量  $Z_{var}$ ;

用于人脸确认的步骤:

在待确认人信息数据库中找到与持卡人智能卡信息对应的样本图片  $x_i$  的投影向量 $Z_{x_i}$ ;

计算 $Z_{x_i}$ 与 $Z_{var}$ 之间的欧氏距离  $D(Z_{x_i}, Z_{var})$ ,

$$D(Z_{x_i}, Z_{var}) = (\sum_{i=1}^M (Z_{x_i} - Z_{var})^2)^{1/2}$$

如果  $D(Z_{x_i}, Z_{var})$  小于设定的阈值则认为持卡人为智能卡的真实主人。

## 联网式多通道门禁考勤系统

### 技术领域

[0001] 本发明涉及一种门禁考勤系统,特别涉及一种联网式多通道门禁考勤系统。

### 背景技术

[0002] 在信息化的今天,社会和个人对安全方便的身份认证技术的需求已变得越来越紧迫。传统的个人身份鉴别主要是通过钥匙、密码、个人身份证明等物理介质,这些的方法的缺陷是容易被窃取而丧失保密的意义。而更严密的安全性往往带来很多不便。在这种情况下,利用人体自身的生物特征进行身份识别成为大势所趋。在众多的生物识别技术中,人脸识别则不需要被识别者配合,适合不希望被鉴别人察觉的场合。而且人脸识别的过程与人类的生物习惯相似,易于被大众接受,所以人脸识别是目前应用最为广泛的生物特征识别技术之一,特别是在非接触环境和不惊动被检测人的情况下,人脸识别技术的优越性远远超过已有的虹膜、指纹等检测方法。

[0003] 目前基于网络的门禁系统的基本组成为摄像机、智能卡读卡机、数据转换模块、网络连接器、中心控制计算机;摄像机采集持卡人的人脸图像,智能读卡机采集持卡人的智能卡信息;数据转换模块将摄像机和智能读卡机采集的视频数据传输到中心控制计算机中;网络接口模块用来进行网络连接;中心控制计算机对持卡人的人脸图像和智能卡信息进行确认和分析识别,从而验证持卡人是否是智能卡的真实主人。若验证持卡人不是智能卡的真实主人,则启动报警系统报警。

[0004] 现有的门禁系统对人脸进行确认和分析识别的软件大多是基于主动形状模型、主动外观模型、主动轮廓模型、主成分分析方法和神经网络的人脸分析和识别算法,这些方法的特点是识别率较高,缺点是算法过于复杂,计算量庞大,分析时间长,若要取得较快的计算时间需要建立在并行计算的硬件系统之上,成本较高。

### 发明内容

[0005] 本发明要解决的技术问题是提供一种成本低、分析识别快的联网式多通道门禁考勤系统。

[0006] 为了解决上述技术问题,本发明的联网式多通道门禁考勤系统包括摄像机、智能卡读卡机、数据转换模块、网络接口模块、中心控制计算机;摄像机采集持卡人的人脸图像,智能读卡机采集持卡人的智能卡信息;数据转换模块将摄像机和智能读卡机采集的视频数据传输到中心控制计算机中;网络接口模块用来进行网络连接;中心控制计算机对持卡人的人脸图像和智能卡信息进行确认和分析识别,从而验证持卡人是否是智能卡的真实主人;

[0007] 所述中心控制计算机的对持卡人的人脸图像和智能卡信息进行确认和分析识别的程序流程包括如下步骤:

[0008] 用于系统上电以后进行自检的步骤;

[0009] 用于采集持卡人的人脸图像和智能卡信息的步骤;

- [0010] 用于对采集来的持卡人的人脸图像进行颜色补偿的步骤；
- [0011] 用于利用基于肤色的人脸检测算法确定人脸的位置，进而截取出人脸图片的步骤；
- [0012] 用于将持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认的子程序；
- [0013] 所述将持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认的子程序包括下述步骤：
- [0014] 用于建立待确认人信息数据库的步骤：
- [0015] 存储每个持卡人的样本图片、智能卡信息和样本图片的投影向量  $Z_{x_i}$ ，所述投影向量  $Z_{x_i}$  按照下述方法得到的：
- [0016] 对存储的每个持卡人的 N 张人脸样本图片  $x_1, x_2, \dots, x_i, \dots, x_N$  进行 Census 变换去除光照影响；将变换后的每幅图像  $x_i$  分为 t 个子块，分别求得各子块的特征向量和特征值；根据设定的各子块的权重，对各子块选取不同数量的特征向量和特征值，组成每幅图像  $x_i$  的变换矩阵  $W_{x_i}$ ，并计算相应的投影向量  $Z_{x_i}$ ；
- [0017] 用于计算持卡人的人脸图片投影向量  $Z_{var}$  的步骤：
- [0018] 将采集的持卡人的人脸图片数据信息  $x_{var}$  进行 Census 变换去除光照影响；将变换后的图像  $x_{var}$  分为 t 个子块，分别求得各子块的特征向量和特征值；根据设定的各子块的权重，对各子块选取不同数量的特征向量和特征值，组成图像  $x_{var}$  的变换矩阵  $W_{x_{var}}$ ，最后求得  $x_{var}$  的投影向量  $Z_{var}$ ；
- [0019] 用于人脸确认的步骤：
- [0020] 在待确认人信息数据库中找到与持卡人智能卡信息对应的样本图片  $x_i$  的投影向量  $Z_{x_i}$ ；
- [0021] 计算  $Z_{x_i}$  与  $Z_{var}$  之间的欧氏距离  $D(Z_{x_i}, Z_{var})$ ，
- $$[0022] D(Z_{x_i}, Z_{var}) = (\sum_{i=1}^M (Z_{x_i} - Z_{var})^2)^{1/2}$$
- [0023] 如果  $D(Z_{x_i}, Z_{var})$  小于设定的阈值则认为持卡人为智能卡的真实主人。
- [0024] 本发明是一种双重验证安防系统，一方面通过非接触性智能卡验证持卡人身份，同时还能根据人脸特征进一步验证持卡人是否是卡的真实主人，这样能够有效的防止冒充他人进入或代人打卡考勤的行为的发生。系统采用基于分块主成分分析的算法，对持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认，计算量较小，分析识别快，适用于海关监控系统，门禁系统，考勤系统等应用方向。将持卡人样本图片和人脸图片分为多个子块，根据表情变化时眼睛、鼻子变化较小，脸部、嘴部变化较大的特点，设定各子块的权重，从而对不同的人脸区域提取不同数量的特征向量，可以有效地减少表情变换对人脸比对和确认的影响。

## 附图说明

- [0025] 下面结合附图和具体实施方式对本发明作进一步详细说明。

- [0026] 图 1 为本发明的联网式多通道门禁考勤系统的结构框图。
- [0027] 图 2 为中心控制计算机的对持卡人的人脸图像和智能卡信息进行确认和分析识别的程序流程图。
- [0028] 图 3 为用于将持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认的子程序流程图。
- [0029] 图 4 为人脸图片和样本图片子块划分示意图。

## 具体实施方式

- [0030] 如图 1 所示,本发明的联网式多通道门禁考勤系统包括门禁终端、数据转换模块、网络接口模块、中心控制计算机。
- [0031] 门禁终端主要包括摄像机和智能卡读卡机,是门禁系统的数据采集模块,所有申请进入的持卡人的面部信息以及智能卡信息都由摄像机和智能读卡机收集。门禁终端还可以包括液晶显示器,液晶显示器可显示采集的持卡人脸部图像,方便持卡人确认图像采集是否正常。
- [0032] 数据转换模块负责将摄像机的视频信号进行 A/D 转换,将采集的图像数据和智能卡信息进行编码、打包,并通过网络进行传输。人脸图像数据量极大,若系统同时监控几个入口,将采集的图像数据传输到中心控制计算机,则需要很高的网络带宽才能满足数据的实时传输要求,同时会给系统的正常工作带来隐患,所以,对图像数据编码是十分必要的。我们选用蛙视公司生产的 VOX-XG2000 多业务光传输平台。数据转换模块还可以采用国内其他公司生产的具有实时编码解码功能的视频传输设备。
- [0033] 网络接口模块:多个入口的图像数据都通过网络接口模块传送给中心控制计算机。网络接口模块的作用是利用网络交换机将多个入口的网络数据汇总,通过网线连接中心控制计算机,传输数据。网络模块采用 VNX-8V-8A(D)-E 系列数字光端机。其通过一根光纤能够同时传输八路视频、八路透明通道(双向音频、双向数据任选)、以太网信号以及电话信号。
- [0034] 中心控制计算机是本发明的联网式多通道门禁考勤系统的核心,它主要完成以下任务:
- [0035] 接收持卡人的图像数据、智能卡信息;
- [0036] 利用本领域公知的方法对采集来的持卡人的人脸图像进行颜色补偿,并利用公知的基于肤色的人脸检测算法确定人脸的位置,进而截取出人脸图片,
- [0037] 将持卡人的人脸图片与人脸数据库中对应的智能卡主人样本图片进行比对和确认。
- [0038] 中心控制计算机采用高性能工作站架构的计算机或其他普通的计算机。
- [0039] 当持卡人与卡主身份不相符时,系统立即发出警报,关闭入口,通知保安人员去往该入口进行处理。
- [0040] 如图 2 所示,门禁系统的软件流程主要包括如下步骤:系统首先进行初始化,设置各种设备的工作模式,进行自检,在自检正常的情况下开始工作,若发现自检出现故障,发送故障信息给管理人员,请求排除故障。开始工作的情况下,首先由要求进入门禁的持卡人提出进入申请;之后,采集持卡人的正面人脸图像和智能卡信息。对采集来的人脸图像进行

颜色补偿,再利用基于肤色的人脸检测算法确定人脸的位置,进而截取出人脸图片。启动将持卡人的人脸图片与数据库中对应的智能卡主人样本图片进行比对和确认的子程序;若两幅人脸图片的相似度满足要求,则认为持卡人确为智能卡主人,开启门禁;若不满足要求,则认为有他人代打卡或冒充卡主的行为发生,立刻启动报警系统。

[0041] 所述将持卡人的人脸图片与待确认人信息数据库中对应的智能卡主人样本图片进行比对和确认的子程序包括下述步骤:

[0042] 用于建立待确认人信息数据库的步骤:

[0043] 存储每个持卡人的样本图片、智能卡信息和样本图片的投影向量 $Z_{x_i}$ ;投影向量 $Z_{x_i}$ 采用下述方法得到:

[0044] 对存储的每个持卡人的N张人脸样本图片 $x_1, x_2, \dots, x_i, \dots, x_N$ 进行Census变换(Ramin Zabih, John Woodfill,《A non-parametric approach to visual correspondence》, IEEE Transactions on Pattern Analysis and Machine Intelligence, 1996)去除光照影响;

[0045] 利用分块的主成分分析算法计算投影向量 $Z_{x_i}$ :将变换后的每幅图像 $x_i$ 分为t个子块,分别求得各子块的特征向量和特征值;如图4所示,设定黑色、灰色、白色子块的权重分别为1、2、4,分别提取黑色、灰色、白色子块的前k个、2k个和4k个特征向量和特征值以组成 $x_i$ 的变换矩阵 $W_{x_i}$ ,计算相应的投影向量 $Z_{x_i}$ 。

[0046] 用于采集持卡人人脸图片和智能卡信息的步骤:

[0047] 用于计算持卡人人脸图片投影向量 $Z_{var}$ 的步骤:

[0048] 将采集的持卡人人脸图片数据信息 $x_{var}$ 进行Census变换去除光照影响;

[0049] 利用分块的主成分分析算法计算投影向量 $Z_{var}$ :将变换后的图像 $x_{var}$ 分为t个子块,分别求得各子块的特征向量和特征值;如图4所示,设定黑色、灰色、白色子块的权重分别为1、2、4,分别提取黑色、灰色、白色子块的前k个、2k个和4k个特征向量和特征值,组成图像 $x_{var}$ 的变换矩阵 $W_{x_{var}}$ ,最后求得 $x_{var}$ 的投影向量 $Z_{var}$ ;

[0050] 用于人脸确认的步骤:

[0051] 在待确认人信息数据库中找到与持卡人智能卡信息对应的样本图片 $x_i$ 的投影向量 $Z_{x_i}$ ;

[0052] 计算 $Z_{x_i}$ 和 $Z_{var}$ 的欧氏距离 $D(Z_{x_i}, Z_{var})$ ,

$$[0053] D(Z_{x_i}, Z_{var}) = (\sum_{i=1}^M (Z_{x_i} - Z_{var})^2)^{1/2}$$

[0054] 如果 $D(Z_{x_i}, Z_{var})$ 小于设定的阈值则认为持卡人为智能卡的真实主人,否则,身份被拒绝;即

[0055]

$$\begin{cases} \text{接受 } x_{var} \text{ 的身份,} & D(Z_{x_i}, Z_{var}) \leq threshold \\ \text{拒绝 } x_{var} \text{ 的身份,} & \text{else} \end{cases}.$$

[0056] 其中,N、t、k的选择没有严格限制,根据硬件能够达到的处理速度,处理能力越强,

N、t、k 值可以选择的越大。本发明根据硬件能够达到的处理速度可以选择 N 为 4、6 或 10，t 可以选择为  $3 \times 5$  个，k 可以选择为 10 或 100。各子块权重的选取不限于上述方式，可以根据表情变化时人脸不同区域变化大小选取。在不考虑表情变换对人脸比对和确认影响的情况下，各子块的权重可以全部选择为 1。

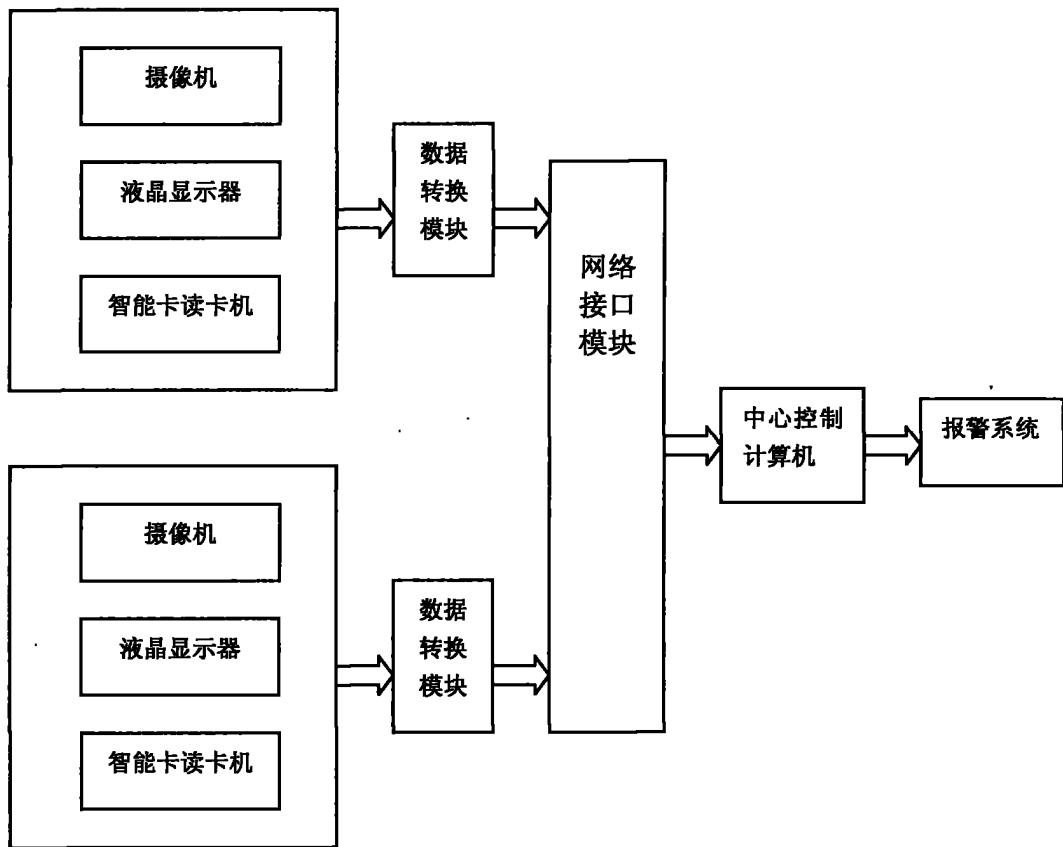


图 1

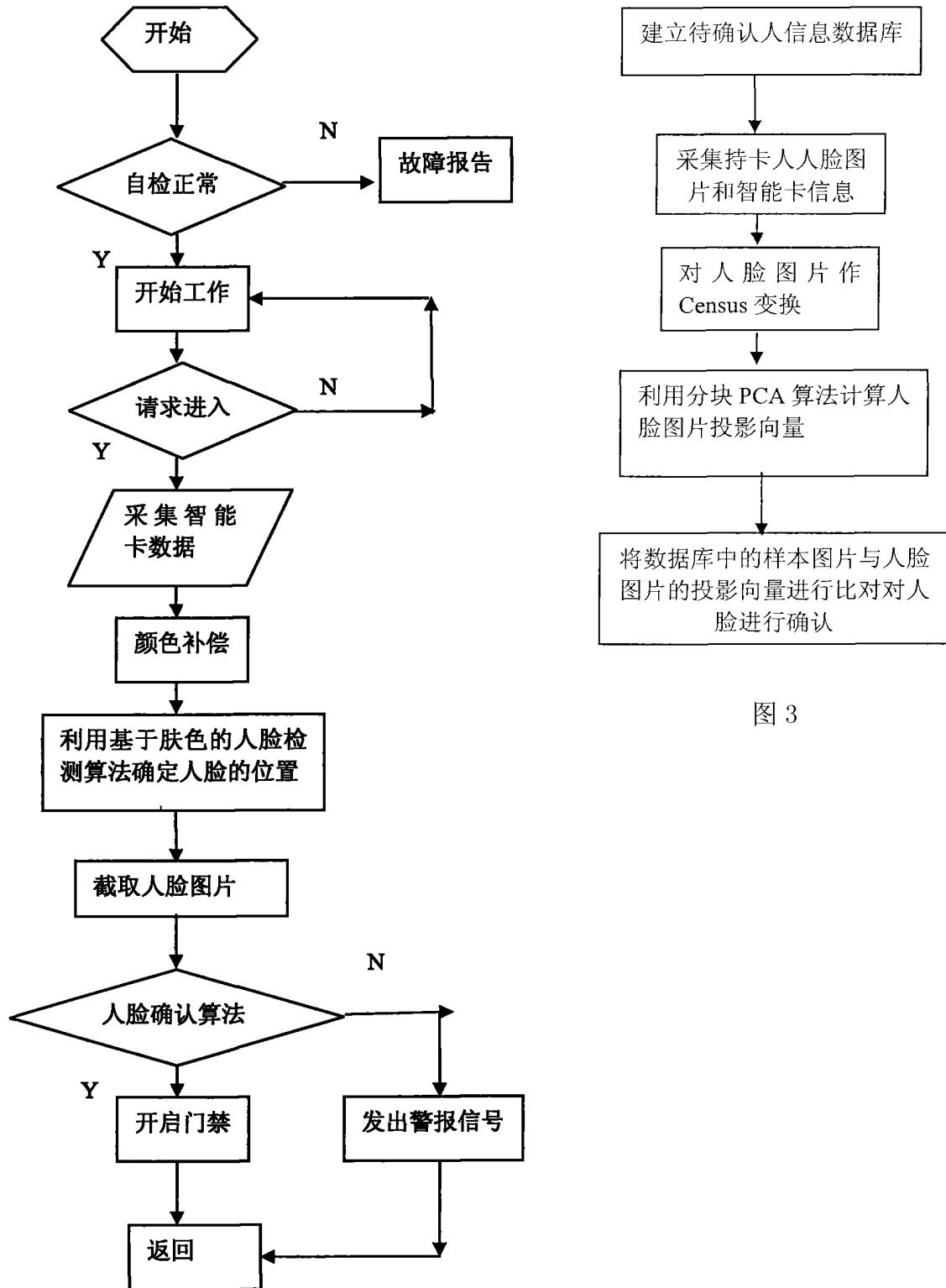


图 2

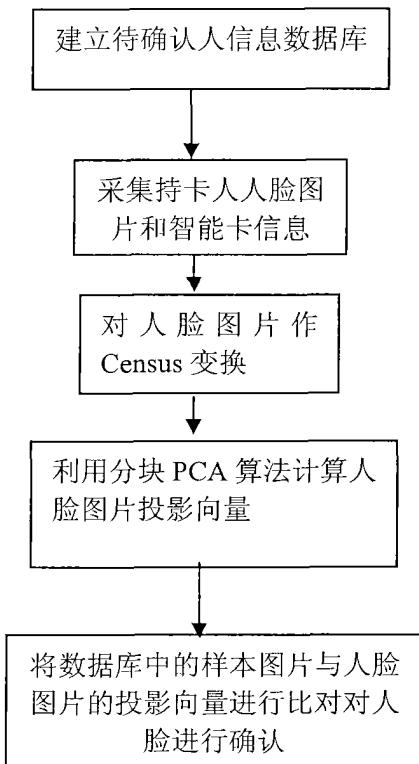


图 3

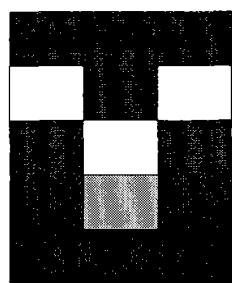


图 4