

[19] 中华人民共和国国家知识产权局



[12] 发明专利说明书

专利号 ZL 200610114291.2

[51] Int. Cl.

A61B 5/117 (2006.01)

G06K 9/62 (2006.01)

G06F 17/00 (2006.01)

[45] 授权公告日 2009 年 6 月 17 日

[11] 授权公告号 CN 100500091C

[22] 申请日 2006.11.3

[21] 申请号 200610114291.2

[73] 专利权人 北京飞天诚信科技有限公司

地址 100083 北京市海淀区学院路 40 号
研 7A 楼 5 层

[72] 发明人 陆 舟 于华章

[56] 参考文献

US2006/0036442 A1 2006.2.16

WO2006/049191 A1 2006.5.11

CN1258346 C 2006.6.7

US2002/0174348 A1 2002.11.21

CN1184771 C 2005.1.12

JP2005-252621 A 2005.9.15

计算机网络安全技术初探. 黄发文. 计算机应用研究. 2002

审查员 高鸿姝

[74] 专利代理机构 北京中海智圣知识产权代理有限公司

代理人 曾永珠

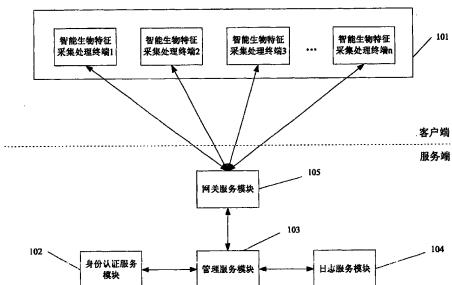
权利要求书 3 页 说明书 8 页 附图 2 页

[54] 发明名称

基于智能生物特征采集处理终端的身份识别
系统和方法

[57] 摘要

本发明公开了一种基于智能生物特征采集处理终端的身份识别系统，包括：智能生物特征采集处理终端、身份认证服务模块，管理服务模块、日志服务模块和网关服务模块。基于上述系统的身份识别方法包括：智能生物特征采集处理终端采集被验证者生物特征信息并进行预处理，再通过网络提交到身份认证服务模块，由身份认证模块与预存相应信息进行比对，并判断接收到的信息是否合法。本发明充分发挥了智能终端资源的作用，减少了网络流量，降低了通讯压力，解决了现有集中式和分布式身份认证的存储和速度瓶颈问题，同时减少了敏感信息泄露的可能性，提高了安全性。



1. 一种基于智能生物特征采集处理终端的分布处理、集中验证的身份识别系统，其特征在于包括：

智能生物特征采集处理终端，所述智能生物特征采集处理终端包含生物特征采集装置或者连接有生物特征采集装置，当生物特征采集装置采集到被验证者的生物特征信息后，所述智能生物特征采集处理终端对该信息进行预处理，所述预处理包括对采集到的原始生物特征信息进行计算、压缩、过滤、提取特征数据、加密和保存的操作，所述智能生物特征采集处理终端内置有加密算法模块，用以采用 RSA、DES、3DES、AES 或 ECC 算法进行所述加密；

身份认证服务模块，将所述智能生物特征采集处理终端传送过来的、经过预处理得到的被验证者身份标识信息与预存的身份标识信息进行比对，在所述身份认证服务模块中包含有解密算法模块，用于对接收到的经过加密的身份标识信息进行解密；

网关服务模块，对身份认证过程中的外部网络访问连接进行控制、过滤。

2. 根据权利要求 1 所述的身份识别系统，其特征在于还包括：

管理服务模块，对身份认证过程进行监控和管理；

日志服务模块，记录身份认证过程中发生的事件。

3. 根据权利要求 1 所述的身份识别系统，其特征在于：所述智能生物特征采集处理终端为内置或外接生物特征采集装置的生物特征采集处理终端。

4. 根据权利要求 2 所述的身份识别系统，其特征在于：所述智能生物特征采集处理终端、身份认证服务模块、管理服务模块、日志服务模块和网关服务模块之间通过网络连接，进行数据通讯。

5. 根据权利要求 4 所述的身份识别系统，其特征在于：所述数据通讯过程中的数据是经过加密的密文数据。

6. 根据权利要求 2 所述的身份识别系统，其特征在于：所述身份认证服务模块、管理服务模块、日志服务模块和网关服务模块可以安装在同一台计算机上，也可以安装在不同计算机上。

7. 一种基于权利要求 1 所述的身份识别系统的分布处理、集中验证的身份识别方法，其特征在于包括以下步骤：

智能生物特征采集处理终端通过其包含或者连接的生物特征采集装置采集被验证者的生物特征信息；

智能生物特征采集处理终端对采集到的生物特征信息进行预处理，所述预处理包括对采集到的原始生物特征信息进行计算、压缩、过滤、提取特征数据、加密和保存的操作，所述加密是采用 RSA、DES、3DES、AES 或者 ECC 算法进行加密；

智能生物特征采集处理终端通过网络将预处理后得到的身份标识信息提交到所述身份认证服务模块；

身份认证服务模块将接收到的身份标识信息进行解密后，与预存的身份标识信息进行比对；

身份认证服务模块判断接收到的身份标识信息是否合法；

其中，在身份认证的过程中，通过网关服务模块对外部网络访问连接进行控制、过滤。

8. 根据权利要求 7 所述的身份识别方法，其特征在于还包括以下步骤：

如果所述身份认证服务模块接收到的身份标识信息是合法的，则向所述智能生物特征采集处理终端发送指令，允许被验证者执行后续操作；

如果所述身份认证服务模块接收到的身份标识信息是不合法的，则向所述智能生物特征采集处理终端发送指令，禁止被验证者执行后续操作，并提示被验证者。

9. 根据权利要求 7 所述的身份识别方法，其特征在于：所述生物特征包括面像、指纹、掌纹、虹膜、声纹、步态、签名。

基于智能生物特征采集处理终端的身份识别系统和方法

技术领域

本发明涉及一种身份识别系统和方法，尤其涉及一种基于智能生物特征采集处理终端的身份识别系统和方法。

背景技术

生物识别技术是指通过计算机利用人体固有的生理特征或者行为特征来进行身份鉴定和认证的过程。由于生物特征识别与传统的密码识别等身份鉴别方法相比，具有很大的优点，因此得到了广泛而深入的研究和应用。目前较常用来进行身份鉴别的生物特征有：面像、指纹、虹膜、声纹、步态、签名等。

随着计算机和网络的快速发展，人们日常的生活娱乐、经济往来，已经与电脑和网络密不可分。数字化生活中的身份识别问题日益逐渐突出。作为娱乐的数字化生活，虚拟的身份可以保护个人。但作为承载经济生活的数字化网络，身份问题却容不得半点虚假。因为网络使面对面的交易变成非面对面的交易，在方便快捷的同时，面对面的安全感和信任感也随之消失。网络还使得面向连接的交易变成非面向连接的交易，双方的在线安全感完全消失。所以身份验证问题，在信息化的今天比过去任何时候都更加重要。因此生物特征识别技术也正在成为未来数字世界身份确认的重要工具。

生物特征识别技术在电子商务中越来越显现重要的地位。电子商务中身份的表示方式也经历了几次发展变革。从最初的“帐号”方式，到后来的“帐号+密码”的方式，以及现有的“数字证书”方式。以上方式均具有容易被泄露、被复制、被传播的缺点，不能很好的满足

识别的唯一性和安全性需要。传统的身份不是人与生俱来的特征，而是系统分配的信物符号。所以传统的身份识别系统只认符号不认人，安全性往往并不能达到要求。随着电子商务、电子政务的发展推进，构建可信任的交易主体表示形式，已经成为交易系统中的基础课题。正因为生物特征的独一无二性、不可抵赖性，以及自身的防伪性，使得采用生物特征作为身份标识将成为主流选择。另外，生物特征具有无需记忆的特点和良好的易用性。在身份识别方面的技术焦点亦将要转变为以生物特征为身份确认信息的生物特征识别技术。

生物特征识别的通常方法是：首先，采集被验证者的生物特征数据；由于采集到的数据量比较大，因此接下来需要从中提取特征值；最后，用特征值和预存的模板信息进行比对，从而完成识别。由于有了生物特征识别技术，数字化生存中的身份确认问题将得到很好地解决。

目前身份认证系统的架构主要包括两种形式，即集中式和分布式。集中式身份认证系统一般在服务器端存储身份识别要素信息，而与其连接的终端只负责完成身份认证信息的采集工作，最终通过网络由服务器端完成信息的识别比对。这种方式要求很高的网络流量，而且大量数据在从终端传输到服务器的过程中容易泄露。另外，由于服务器需要首先完成预处理的工作，然后才能进行比对，造成比对速度较慢。分布式身份认证系统一般在终端上完成完整的身份识别验证，包括身份认证信息的采集和比对等操作，无需服务器的参与。验证通过后，才允许被验证者访问网络资源。但是，一般的终端配置较低，难以存储大量数据，因此识别过程将非常耗时。

发明内容

本发明旨在提供一种基于智能生物特征采集处理终端的集中分

布式身份识别的系统和方法，解决现有集中式和分布式身份认证系统存在的不足。

本发明的技术方案如下：基于智能生物特征采集处理终端的身份识别系统包括：

智能生物特征采集处理终端，采集和预处理被验证者生物特征信息；

身份认证服务模块，将所述智能生物特征采集处理终端传送过来的、经过预处理得到的被验证者身份标识信息与预存的身份标识信息进行比对。

所述系统还包括：

管理服务模块，对身份认证过程进行监控和管理；

日志服务模块，记录身份认证过程中发生的事件；

网关服务模块，对身份认证过程中的外部网络访问连接进行控制、过滤。

其中，所述智能生物特征采集处理终端内置或外接生物特征采集装置的生物特征采集处理终端。

所述智能生物特征采集处理终端、身份认证服务模块、管理服务模块、日志服务模块和网关服务模块之间通过网络连接，进行数据通讯。

所述数据通讯过程中的数据是经过加密的密文数据。

所述身份认证服务模块、管理服务模块、日志服务模块和网关服务模块可以安装在同一台计算机上，也可以安装在不同计算机上。

基于智能生物特征采集处理终端的身份识别系统的身份识别方法，包括以下步骤：

智能生物特征采集处理终端采集被验证者生物特征信息；

智能生物特征采集处理终端对采集到的生物特征信息进行预处理；

智能生物特征采集处理终端通过网络将预处理后得到的身份标识信息提交到所述身份认证服务模块；

身份认证服务模块将接收到的身份标识信息与预存的相应信息进行比对；

身份认证服务模块判断接收到的身份标识信息是否合法。

所述方法进一步包括以下步骤：

如果所述身份认证服务模块接收到的身份标识信息是合法的，则向所述智能生物特征采集处理终端发送指令，允许被验证者执行后续操作；

如果所述身份认证服务模块接收到的身份标识信息是不合法的，则向所述智能生物特征采集处理终端发送指令，禁止被验证者执行后续操作，并提示被验证者。

所述预处理包括对采集到的原始生物特征信息进行计算、压缩、过滤、提取特征数据、加密或保存的操作。

所述生物特征包括面像、指纹、掌纹、虹膜、声纹、步态、签名。

与现有技术相比，本发明的有益效果是：

1. 充分发挥了智能终端资源的作用，减少了网络流量，降低了通讯压力，提升了系统部署的灵活性；
2. 解决现有集中式和分布式身份认证的存储和速度瓶颈问题。
3. 减少了通讯过程中敏感信息泄露的可能性，提高了安全性；

附图说明

图 1 是本发明所述的身份识别系统结构图；

图 2 是本发明所述的身份识别方法流程图。

具体实施方式

下面结合附图和具体实施例对本发明的系统和方法进行更详细的描述。

图 1 为本发明所述的基于智能生物特征采集处理终端的身份识别系统结构图。

参考图 1，身份识别系统包括：智能生物特征采集处理终端 101、身份认证服务模块 102、管理服务模块 103、日志服务模块 104 和网关服务模块 105。所述智能生物特征采集处理终端、身份认证服务模块、管理服务模块、日志服务模块和网关服务模块之间通过网络连接，进行数据通讯。

其中所述智能生物特征采集处理终端 101 可能包括智能生物特征采集处理终端 1、智能生物特征采集处理终端 2、智能生物特征采集处理终端 3、……若干个相对独立的终端，它们用于采集和预处理被验证者的生物特征信息。这里的被验证者的生物特征信息可以为面像、指纹、掌纹、虹膜、声纹、步态、签名等信息。所述智能生物特征采集处理终端 101 包含生物特征采集装置，或连接有生物特征采集装置。当生物特征采集装置采集到被验证者的生物特征信息后，对应的智能生物特征采集处理终端对该信息进行预处理。这里的预处理包括计算、提取特征数据、比较和保存等，然后经过预处理的被验证者的身份标识信息通过网络被传输到身份验证服务模块 102。为了确保数据传输安全，所述智能生物特征采集处理终端 101 或生物特征采集装置内置有加密算法，如 RSA、DES、3DES、AES 或 ECC 等，可以对数据进行加密。相应地，身份认证服务端含有对应的解密算法。在接收到被验证者的加密身份标识信息后，身份认证服务模块 102 将对该信息进行解密，然后将其与数据库中预存的相应信息进行比对。如

果有匹配项，则说明被验证者为合法用户，系统将允许其进行下一步操作。否则，系统将拒绝其执行下一步的操作。管理服务模块 103 在整个认证过程中发挥控制和协调的作用，管理员可以使用管理服务模块 103 来监控身份认证服务模块 102 和日志服务模块 104 的运行情况。日志服务模块 104 用于对整个认证过程中发生的各种事件进行记录，以便将来进行查询和分析等活动。网关服务模块 105 用于控制、过滤外部网络连接访问。

身份认证服务模块 102、管理服务模块 103、日志服务模块 104 和网关服务模块 105 可以安装在不同计算机上—这些计算机分别作为身份认证服务器、管理服务器、网关服务器和日志服务器；也可以安装在同一台计算机服务器上。网关服务模块 105 或网关服务器不是必需的。

图 2 是本发明基于智能生物特征采集处理终端的身份识别方法流程图。

参考图 2，身份识别方法包括如下步骤：

步骤 201，智能生物特征采集处理终端采集被验证者的生物特征信息。智能生物特征采集处理终端通过内置或与其连接的生物特征采集装置采集被验证者的生物特征信息。所述生物特征信息可以为面像、指纹、掌纹、虹膜、声纹、步态、签名等信息。目前，市场上用于对上述生物特征信息进行采集的装置很多。例如，可以通过指纹传感器来采集指纹信息。

步骤 202，智能生物特征采集处理终端对采集到的生物特征信息进行预处理。在这个过程中，智能生物特征采集处理终端可以对步骤 201 中采集到的原始生物特征信息进行计算、过滤、压缩、提取生物特征数据、比较、加密和保存等操作。

步骤 203，智能生物特征采集处理终端通过网络将预处理后得到的信息提交到身份认证服务模块。智能生物特征采集处理终端通过网络连接先将预处理后得到的身份标识信息（特征值）传送到网关服务模块，再经过网关服务模块将上述信息传送管理服务模块。然后，通过管理服务模块将信息传送到身份认证服务模块。

步骤 204，身份认证服务模块将接收到的信息与预存的信息进行比对。身份认证服务模块对接收到的身份标识信息首先进行处理，包括解密、解压缩等操作，然后将最终得到的结果与数据库中预存的相应信息进行比对。

步骤 205，身份认证服务模块判断接收到的信息是否合法。如果没有发现匹配项，则说明该信息不合法，转到步骤 206；如果身份认证服务模块发现匹配项，则说明该信息合法，转到步骤 207。

步骤 206，向智能生物特征采集处理终端发送指令，禁止被验证者执行后续操作，并提示被验证者。身份认证服务模块通过网络连接向智能生物特征采集处理终端发送指令，禁止被验证者继续执行操作，并在智能生物特征采集处理终端提示被验证者出错。例如，可以要求被验证者重新输入生物特征或向管理员登记生物特征。

步骤 207，向智能生物特征采集处理终端发送指令，允许被验证者执行后续操作。验证通过，身份认证服务模块网络向智能生物特征采集处理终端发送指令，允许被验证者继续执行操作。

在步骤 206 和 207 中，身份认证服务模块比对判断结果发送给管理服务模块后由管理服务模块通过网关服务模块向智能生物特征采集处理终端发送相应的指令。在整个认证过程中，可以使用日志服务模块来记录各种事件，包括认证成功、认证失败等信息，以便对整个认证过程进行监控和管理。

所述系统和方法可以应用于有多个管理员和多台游戏机的游戏经营场所。例如，在每台游戏机上配备一个指纹识别装置。所有管理员的指纹特征信息均存储在指纹认证服务器上。管理员执行操作之前，必须先在游戏机终端上扫描指纹。然后，游戏机终端将经过预处理的管理员指纹特征信息提交到指纹认证服务器。指纹认证服务器对指纹信息进行认证，并将结果返回给游戏机终端，同时将认证结果以及相关信息记录到日志服务器。另外，系统还配有一台管理服务器，即安装了指纹管理服务程序的 PC，用于执行管理员指纹的登记、修改和删除等操作。如果认证通过，则允许管理员对终端执行操作。否则，系统拒绝管理员对终端执行任何操作。其中，管理服务器由游戏经营场所的负责人或指定的超级管理员控制。为了确保管理服务器不被非法使用，也可以为其配备一个指纹识别装置。

以上所述实施方式仅为本发明的优选实施例，本发明不限于上述实施例，对于本领域一般技术人员而言，在不背离本发明原理的前提下对它所做的任何显而易见的改动，都属于本发明的构思和所附权利要求的保护范围。

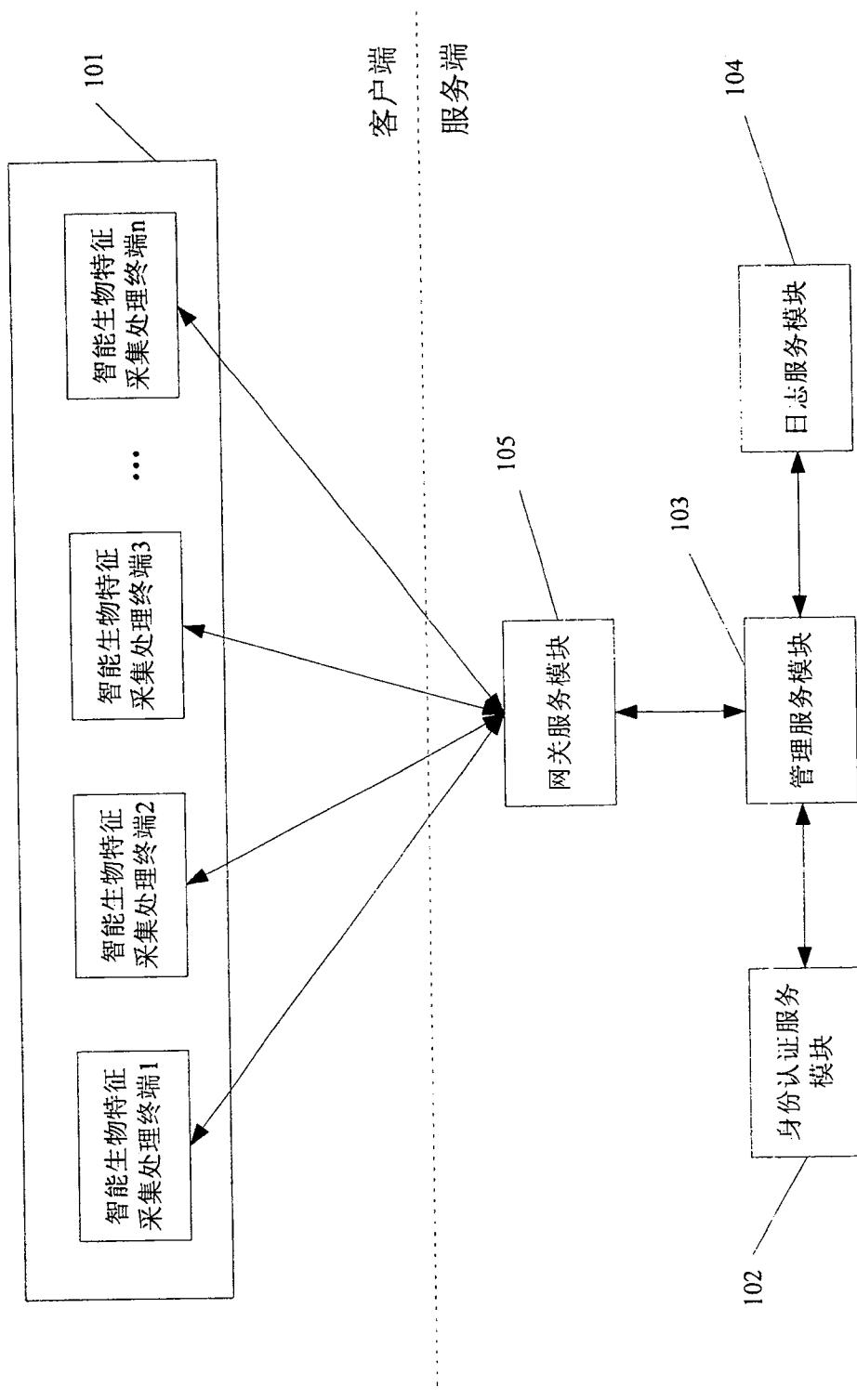


图 1

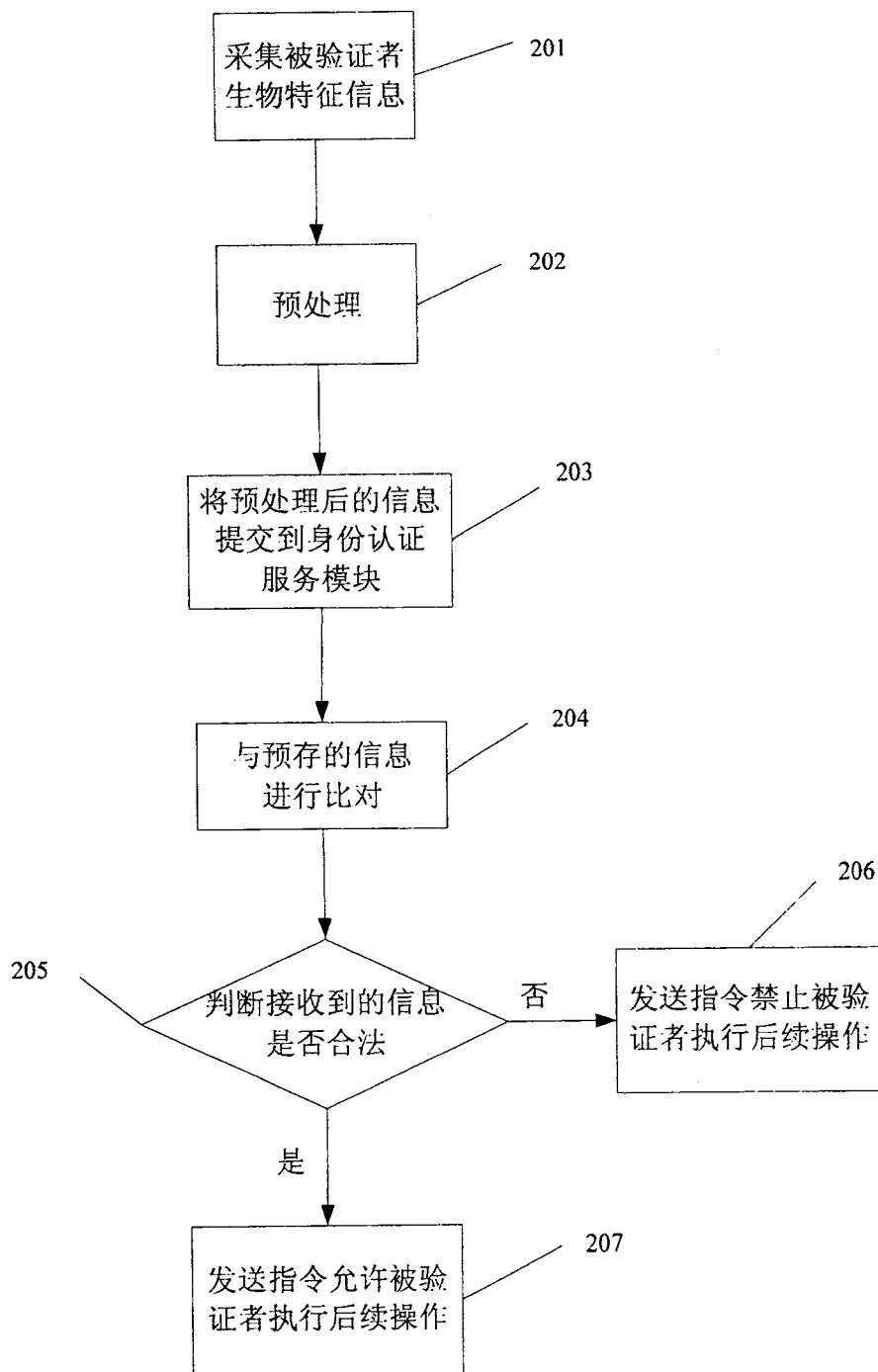


图 2