(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 1945554 B
(45)授权公告日 2011.04.27

(21)申请号 200610113676.7

(22)申请日 2006.10.12

(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

(74)专利代理机构 北京集佳知识产权代理有限公司 11227
代理人 孙长龙

(51)Int.Cl.
G06F 12/14(2006.01)
G06F 21/00(2006.01)
G06Q 30/00(2006.01)
H04L 9/32(2006.01)

(56)对比文件
CN 1364276 A,2002.08.14, 说明书第5页第15行至第20行, 第7页第6行至第30行.
US 5872834 A,1999.02.16, 全文.

审查员 王燕

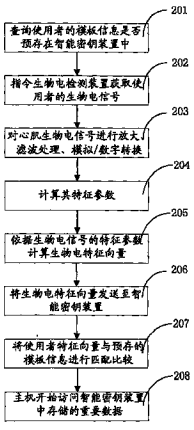
权利要求书 3 页 说明书 8 页 附图 4 页

(54)发明名称

一种提高智能密钥安全性的方法及装置

(57)摘要

本发明公开了一种提高智能密钥装置安全性的方法,包括:对主机使用者进行生物电信号检测;确认该使用者身份后,允许主机访问智能密钥装置中存储的数据。本发明按下述步骤,对主机使用者进行生物电信号检测:获取使用者的生物电信号;将所述生物电信号处理成生物电特征向量;将所述生物电特征向量与预存的相应特征向量模板进行匹配比较;如匹配比较结果超过预设的门限值,确认该使用者。本发明同时还提供两种提高智能密钥安全性的装置。本发明消除了智能密钥装置在对使用者身份鉴定方面存在的安全隐患,提高其可靠性和安全性。



CN 1945554 B

1. 一种提高智能密钥安全性的方法，其特征在于，包括：

对主机使用者进行心肌生物电信号和脑电波信号检测；

确认该使用者身份后，允许主机访问智能密钥装置中存储的数据；

按下述步骤对主机使用者进行生物电信号检测：

获取使用者的生物电信号；

将所述生物电信号处理成生物电特征向量；

将所述生物电特征向量与预存的相应特征向量模板进行匹配比较；

如匹配比较结果超过达到预设条件，确认该使用者；

按下述步骤将所述生物电信号处理成生物电特征向量：

将获取的生物电信号进行处理，包括放大处理、滤波处理、模 / 数转换；

在处理后的生物电信号中提取生物电特征参数，依据所述生物电特征参数计算出生物电特征向量；

所述在处理后的生物电信号中提取生物电特征参数包括：

计算生物电信号一个波形周期中的斜率；

计算生物电信号一个波形周期中峰值时间；

计算生物电信号周期波形内采样点值的方差；

计算生物电信号周期波形的高阶矩；

计算生物电信号周期波形的协方差。

2. 根据权利要求 1 所述的方法，其特征在于，所述达到预设条件包括将被鉴定者的生物电信号和预先设定的门限值进行比较，若比较结果超过所述预设的门限值，则确认该被鉴定者身份合法。

3. 根据权利要求 2 所述的方法，其特征在于，所述计算生物电信号一个波形周期中的斜率包括：计算生物电信号中每一个周期内生物电信号的波形从起始点到第一个波峰的上升斜率；从第一个波谷到第二个波峰的上升斜率；从波峰到最低点的下降斜率；最后一个波峰的上升斜率。

4. 根据权利要求 2 所述的方法，其特征在于，所述计算生物电信号一个波形周期中峰值时间包括：计算每一个周期内生物电信号的波形从起点到第一个波峰所用的时间；从第一个波峰到最后一个波峰所用的时间。

5. 根据权利要求 2 所述的方法，其特征在于，所述计算生物电信号周期波形内采样点值的方差包括：计算前 n 个周期波形信号内采样点值的方差，并计算出 n 个方差的平均值。

6. 根据权利要求 2 所述的方法，其特征在于，所述计算生物电信号周期波形的高阶矩包括：计算前 n 个周期波形信号中每个周期的 4 阶矩，并计算出前 n 个波形信号周期 4 阶矩的平均值。

7. 根据权利要求 2 所述的方法，其特征在于，所述计算生物电信号周期波形的协方差包括：计算前 n 个周期波形信号相邻两周期的协方差。

8. 根据权利要求 2 所述的方法，其特征在于，根据上述特征参数生成特征向量。

9. 根据权利要求 8 所述的方法，其特征在于，所述根据上述特征参数生成特征向量的方法是将特征参数按一定的顺序排列。

10. 根据权利要求 1 所述的方法，其特征在于，采用矢量量化法、隐马尔可夫模型法、动

态时间规整法或神经网络法进行匹配比较。

11. 根据权利要求 1 所述的方法，其特征在于，所述获取使用者生物电信号包括：

获取使用者的生物电信号，同时获取使用者电阻、体温、脉搏与 / 或湿度信号；

将电阻、体温、脉搏与 / 或湿度信号与上述生物电信号共同作为被鉴定者的生物电信号。

12. 根据权利要求 1 至 11 任一项所述的方法，其特征在于，所述生物电信号包括心肌生物电信号和脑电波信号。

13. 根据权利要求 1 至 11 任一项所述的方法，其特征在于，所述生物电信号的通过测量人体两手之间的电位差获取。

14. 一种提高智能密钥安全性的装置，其特征在于，包括：

生物电检测单元，用于获取主机使用者的心肌生物电信号和脑电波信号，并将生物电信号处理成生物电特征向量；

智能密钥单元，用于将上述生物电特征向量同预存的该使用者的特征向量模板进行匹配比较，如符合要求，则允许被访问；

所述生物电检测单元包括：

获取单元，用于获取主机使用者的生物电信号；

信号处理单元，用于将所述生物电信号处理成生物电特征向量；

按下述步骤将所述生物电信号处理成生物电特征向量：

将获取的生物电信号进行处理，包括放大处理、滤波处理、模 / 数转换；

在处理后的生物电信号中提取生物电特征参数，依据所述生物电特征参数计算出生物电特征向量；

所述在处理后的生物电信号中提取生物电特征参数包括：

计算生物电信号一个波形周期中的斜率；

计算生物电信号一个波形周期中峰值时间；

计算生物电信号周期波形内采样点值的方差；

计算生物电信号周期波形的高阶矩；

计算生物电信号周期波形的协方差。

15. 根据权利要求 14 所述的装置，其特征在于，还包括：

状态指示单元，用于显示各种处理状态。

16. 根据权利要求 14 所述的装置，其特征在于，所述智能密钥单元包括：

确认单元，用于将所述生物电特征向量与预存的相应特征向量模板进行匹配比较，如符合要求，则允许主机操作存储单元内数据。

17. 如权利要求 14 所述的装置，其特征在于，所述主机对存储单元内数据进行操作包括读、写、加 / 解密处理。

18. 一种提高智能密钥安全性的装置，其特征在于，包括：

生物电信号采集器，用于获取主机使用者的心肌生物电信号和脑电波信号；

存储器，用于存储特征向量模板信息和其它数据；

处理器，用于将上述生物电信号处理成生物电特征向量，并将该生物电特征向量与预存在存储器内相应的特征向量模板进行匹配比较，如符合要求，则允许主机访问存储器内

数据；

按下述步骤将所述生物电信号处理成生物电特征向量：

将获取的生物电信号进行处理，包括放大处理、滤波处理、模 / 数转换；

在处理后的生物电信号中提取生物电特征参数，依据所述生物电特征参数计算出生物电特征向量；

所述在处理后的生物电信号中提取生物电特征参数包括：

计算生物电信号一个波形周期中的斜率；

计算生物电信号一个波形周期中峰值时间；

计算生物电信号周期波形内采样点值的方差；

计算生物电信号周期波形的高阶矩；

计算生物电信号周期波形的协方差。

一种提高智能密钥安全性的方法及装置

技术领域

[0001] 本发明涉及智能密钥领域，特别是涉及一种提高智能密钥安全性的方法及装置。

背景技术

[0002] 随着互联网技术与电子商务的快速发展，越来越多的商务活动转移到网络上开展，面对面的商业交易正被不见面的网上交易代替。政府部门为提高办公效率，也将互联网技术引入工作之中，使政务信息得以高速传输。为保证网络信息的安全，必须对其使用者进行严格的身份认证，通过后，才允许该使用者读取或发送重要数据。

[0003] 现有技术在主机上加设智能密钥装置，该智能密钥装置中存储重要数据，通过数据通信接口与主机相连接，需使用者输入预设的密码后，智能密钥装置才允许主机读取其内存储的重要数据。但是密码仅为一组简单的数据，他人可以通过窥视、密码破译等手段非法获取该密码，造成智能密钥装置内保存的重要数据外泄。

[0004] 为增强智能密钥装置的安全性，现有技术在智能密钥装置上加设指纹认证装置，使用者需通过指纹认证后，方可读取智能密钥装置内的重要数据。

[0005] 请参阅图 1，为现有提高智能密钥装置安全性的方法流程图，具体步骤如下：

[0006] 101、在智能密钥装置中预置所有可能的使用者的指纹，指纹按使用者标识号码存储在智能密钥装置的数据库中；

[0007] 102、使用者在指纹认证装置上输入其标识号码和指纹信息；

[0008] 103、指纹认证装置根据输入的标识号码调出相应的指纹，与输入的使用者指纹相比较；

[0009] 104、比较结果符合要求，则确认该使用者身份合法，发送确认信息至智能密钥装置；

[0010] 105、智能密钥装置接收到该确认信息后，允许主机读取其内存储的重要数据。

[0011] 该方法使用指纹认证增强智能密钥装置的安全性，但是指纹可以采用生物技术进行仿制，也能在乳胶中隐去，使该智能密钥装置在对使用者身份鉴定方面存在一定的安全隐患，其可靠性和安全性尚存缺陷。

发明内容

[0012] 有鉴于此，本发明提供一种提高智能密钥安全性的方法及装置，解决智能密钥在对使用者身份鉴定方面存在的安全隐患，提高其可靠性和安全性。

[0013] 本发明一种提高智能密钥安全性的方法，包括：对主机使用者进行生物电信号检测；确认该使用者身份后，允许主机访问智能密钥。

[0014] 优选的，按下述步骤，对主机使用者进行生物电信号检测；获取使用者的生物电信号；将所述生物电信号处理成生物电特征向量；将所述生物电特征向量与预存的相应特征向量模板进行匹配比较；如匹配比较结果超过达到预设条件，确认该使用者。

[0015] 优选的，所述达到预设条件包括将被鉴定者的生物电信号和预先设定的门限值进

行比较，若比较结果超过所述预设的门限值，则确认该被鉴定者身份合法。

[0016] 优选的，按下述步骤，将所述生物电信号处理成生物电特征向量：将获取的生物电信号进行处理，包括放大处理、滤波处理、模／数转换；在处理后的生物电信号中提取生物电特征参数，依据所述生物电特征参数计算出生物电特征向量。

[0017] 优选的，所述在处理后的生物电信号中提取生物电特征参数包括：

[0018] 计算生物电信号一个波形周期中的斜率；

[0019] 计算生物电信号一个波形周期中峰值时间；

[0020] 计算生物电信号周期波形内采样点值的方差；

[0021] 计算生物电信号周期波形的高阶矩；

[0022] 计算生物电信号周期波形的协方差。

[0023] 优选的，所述计算生物电信号一个波形周期中的斜率，包括：计算生物电信号中每一个周期内生物电信号的波形从起始点到第一个波峰的上升斜率；从第一个波谷到第二个波峰的上升斜率；从波峰到最低点的下降斜率；最后一个波峰的上升斜率。

[0024] 优选的，所述计算生物电信号一个波形周期中峰值时间包括：计算每一个周期内生物电信号的波形从起点到第一个波峰所用的时间；从第一个波峰到最后一个波峰所用的时间；

[0025] 优选的，所述计算生物电信号周期波形内采样点值的方差包括：计算前 n 个周期波形信号内采样点值的方差，并计算出 n 个方差的平均值。

[0026] 优选的，所述计算生物电信号周期波形的高阶矩包括：计算前 n 个周期波形信号中每个周期的 4 阶矩，并计算出前 n 个波形信号周期 4 阶矩的平均值。

[0027] 优选的，所述计算生物电信号周期波形的协方差包括：计算前 n 个周期波形信号相邻两周期的协方差。

[0028] 优选的，根据上述特征参数生成特征向量。

[0029] 优选的，所述根据上述特征参数生成特征向量的方法是将特征参数按一定的顺序排列。

[0030] 优选的，采用矢量量化法、隐马尔可夫模型法、动态时间规整法或神经网络法进行匹配比较。

[0031] 优选的，所述获取使用者生物电信号包括：获取使用者的生物电信号，同时获取使用者电阻、体温、脉搏与／或湿度信号；将电阻、体温、脉搏与／或湿度信号与上述生物电信号共同作为被鉴定者的生物电信号。

[0032] 优选的，所述生物电信号包括心肌生物电信号和脑电波信号。

[0033] 优选的，所述生物电信号的通过测量人体两手之间的电位差获取。

[0034] 本发明一种提高智能密钥安全性的装置，包括：生物电检测单元，用于获取主机使用者的生物电信号，并将生物电信号处理成生物电特征向量；智能密钥单元，用于将上述生物电特征向量同预存的该使用者的特征向量模板进行匹配比较，如符合要求，则允许被访问。

[0035] 优选的，还包括：状态指示单元，用于显示各种处理状态。

[0036] 优选的，所述生物电检测单元包括：获取单元，用于获取主机使用者的生物电信号；信号处理单元，用于将所述生物电信号处理成生物电特征向量。

[0037] 优选的，所述智能密钥单元包括：确认单元，用于将所述生物电特征向量与预存的相应特征向量模板进行匹配比较，如符合要求，则允许主机操作存储单元内数据；

[0038] 优选的，所述主机对存储单元内数据进行操作包括读、写、加／解密处理。存储单元，用于存储特征向量模板信息和其它数据。

[0039] 本发明一种提高智能密钥安全性的装置，包括：生物电信号采集器，用于获取主机使用者的生物电信号；存储器，用于存储特征向量模板信息和其它数据；处理器，用于将上述生物电信号处理成生物电特征向量，并将该生物电特征向量与预存在存储器内相应的特征向量模板进行匹配比较，如符合要求，则允许主机访问存储器内数据。

[0040] 与现有技术相比，本发明具有以下优点：

[0041] 本发明首先对主机使用者进行人体生物特征认证，通过后智能密钥装置允许主机读取其内保存的重要数据。因每个人的生物特征都是独有的，不同人之间生物特征的重复性可以忽略不计，并且无仿制、伪造的可能。因此，通过对使用者的生物特征进行鉴定，可提高智能密钥装置的可靠性和安全性。

附图说明

[0042] 图 1 为现有提高智能密钥装置安全性的方法流程图；

[0043] 图 2 为本发明提高智能密钥安全性的方法实施例的流程图；

[0044] 图 3 为人体心肌生物电信号在一个周期电位差随时间的变化示意图；

[0045] 图 4 为使用者的心肌生物电信号的波形图；

[0046] 图 5 为使用者的心肌生物电信号的波形图；

[0047] 图 6 为对人体心肌生物电信号的主要特征参数检测示意图；

[0048] 图 7 为本发明提高智能密钥安全性的装置一实施例示意图；

[0049] 图 8 为本发明提高智能密钥安全性的装置另一实施例示意图。

具体实施方式

[0050] 为使本发明的上述目的、特征和优点能够更加明显易懂，下面结合附图和具体实施方式对本发明作进一步详细的说明。

[0051] 本发明的核心思想是首先对主机使用者进行人体生物特征认证，通过后智能密钥装置允许主机读取其内保存的重要数据。因每个人的生物特征都是独有的，不同人之间生物特征的重复性可以忽略不计，并且无仿制、伪造的可能。因此，通过对使用者的生物特征进行鉴定，可提高智能密钥装置的可靠性和安全性，做到万无一失。

[0052] 生物电是生物体所呈现的电现象。产生生物电的基础来自细胞膜内外的电位差。安静时，细胞内处于负电位，细胞外处于负电位，称“静息电位”；兴奋时，瞬间细胞内的电位升高并超过了细胞外而相对地变成了正电位，暂时可变为内正外负，称“动作电位”，这种电位的变化只持续几毫秒，兴奋过后又恢复原来的状态。脑和心脏等器官所表现的复杂电变化，是它们的组成细胞电变化的总和，单个个体的生物电信号基本一致，不同个体的生物电信号存在较大的差异。

[0053] 基于生物特征的身份鉴定是采用每个人独一无二的生物特征来验证其身份的合法性。从理论上说，生物特征认证是最可靠的身份认证方式，因为它直接使用人体内的生物

特征信号来表示每一个人的身份，不同的人具有相同生物特征的可能性可以忽略不计，并且不可能被仿冒，因此，具有极高的可靠性和安全性。

[0054] 本发明在智能密钥装置中增加生物电信号检测装置，主机通过智能密钥装置控制生物电信号检测装置获取使用者的生物电信号，经处理后与智能密钥装置中预存的生物电模板信息进行匹配比较，通过后，智能密钥装置允许主机访问其内存储的重要数据。

[0055] 本发明通过专用的仪器获取使用者生物电信号，生物电信号可以为人体心肌生物电信号、脑电波信号等有较强特征的信号量。再将获取使用者的生物电信号进行放大、滤波处理后，在处理后的图形进行特殊点 A/D（模／数）转换，提取交易者生物电信号的特征参数，然后根据生物电特征参数计算生成使用者的生物电特征向量。

[0056] 本发明将交易者的生物电特征向量发送至智能密钥装置，智能密钥装置将该生物电特征向量与预先存储在数据库中的该使用者的特征模板进行匹配比较。当匹配达到或超过预设的门限值时，确认交易者身份合法；当匹配没有达到或超过预设的门限值时，确认交易者身份非法。

[0057] 本发明将确认结果信息发送至主机，主机开始访问智能密钥装置中存储的重要数据，智能密钥确认使用者身份合法后，允许主机访问受保护的重要数据。

[0058] 参阅图 2，为本发明提高智能密钥安全性的方法实施例的流程图，具体步骤如下：

[0059] 步骤 201、查询主机使用者的生物电特征向量模板信息是否预存在智能密钥装置中；

[0060] 主机使用者在主机上输入自己的标识号码，主机发送查询该使用者生物电特征向量模板信息的指令到智能密钥装置，该指令包含使用者输入的标识号码。智能密钥装置根据标识号码查找相应的特征向量模板信息是否已经预存到其装置中，并将查询结果返回主机。

[0061] 如使用者特征向量模板信息还没有预存到智能密钥装置中，主机将终止进行后续操作，并向持有人显示一个错误信息；如使用者生物电信息已经预存到智能密钥装置中，执行步骤 202。

[0062] 步骤 202、主机通过智能密钥装置指令生物电检测装置获取使用者的生物电信号；

[0063] 生物电信号优选为心肌生物电信号。获取时需要用指夹式生物电信号检测器固定在交易者的指端，利用测量人体两手之间的电位差获取心肌生物电信号。

[0064] 人体心肌生物电是由心脏的窦房结发出的一次兴奋，按一定的途径和进程，依次传向心房和心室，引起整个心脏的兴奋；因此，每一个心动周期中，心脏各部分兴奋过程中出现的电变化传播方向、途径、次序和时间等都有一定的规律。这种生物电变化通过心脏周围的导电组织和体液，反映到身体表面，使身体各部位在每一心动周期中也都发生有规律的电变化。将测量电极放置在人体表面的一定部位记录出来的心脏电变化曲线能够反映心脏兴奋的产生、传导和恢复过程中的生物电变化系。而该变化曲线反映的人体生物电信号在经过生物电放大器的放大后，能够被检测出来。

[0065] 请参阅图 3，图 3 为人体心肌生物电信号在一个周期电位差（y 轴）随时间（t 轴）的变化示意图，该图所示波形是一个典型的生物电信号的波形图。图 4、图 5 为两个不同使用者的心肌生物电信号的波形图，经对比可以看出，虽然每个个体的心肌生物电信号的特

征会随着检测部位和检测时刻的变化而有所差异，但是，同一个人的心肌生物电信号基本保持稳定，不同个体的心肌生物电信号却存在比较大的差异。因此，通过心肌生物电信号比较容易识别不同个体。

[0066] 步骤 203、对生物电信号进行放大、滤波处理、模拟 / 数字信号的转换 ；

[0067] 将采集到的生物电信号通过信号放大器进行放大，并将放大后的生物电信号进行滤波处理。

[0068] 步骤 204、对处理后的生物电信号进行特殊点检测，并计算其特征参数 ；

[0069] 生物电特征参数的提取是指提取生物电信号信号中表征人的基本特征，选取的特征必须能够有效地区分不同的交易者，且对同一交易者的变化保持相对稳定，同时要求特征参数计算简便，最好有高效快速算法，以保证识别的实时性。

[0070] 图 6 为对人体心肌生物电信号的主要特征参数检测示意图，生物电信号的特征参数包括生物电信号的顶点和谷点，与之相对的特征参数包括 ：上升及下降斜率 k1、k2、k3、k4，时间间隔 t1、t2，具体表现为 ：

[0071] 计算生物电信号一个波形周期中的斜率 ；

[0072] 计算生物电信号一个波形周期中峰值时间 ；

[0073] 计算生物电信号周期波形内采样点值的方差 ；

[0074] 计算生物电信号周期波形的高阶矩 ；

[0075] 计算生物电信号周期波形的协方差。

[0076] 所述计算生物电信号一个波形周期中的斜率包括 ：计算生物电信号中每一个周期内生物电信号的波形从起始点到第一个波峰的上升斜率 ；从第一个波谷到第二个波峰的上升斜率 ；从波峰到最低点的下降斜率 ；最后一个波峰的上升斜率 ；

[0077] 所述计算生物电信号一个波形周期中峰值时间包括 ：计算每一个周期内生物电信号的波形从起点到第一个波峰所用的时间 ；从第一个波峰到最后一个波峰所用的时间 ；

[0078] 所述计算生物电信号周期波形内采样点值的方差包括 ：计算前 n 个周期波形信号内采样点值的方差，并计算出 n 个方差的平均值 ；

[0079] 所述计算生物电信号周期波形的高阶矩包括 ：计算前 n 个周期波形信号中每个周期的 4 阶矩，并计算出前 n 个波形信号周期 4 阶矩的平均值。

[0080] 所述计算生物电信号周期波形的协方差包括 ：计算前 n 个周期波形信号相邻两周期的协方差。其中，n 大于 1。

[0081] 在计算出以上这些特征参数后，只需利用特征向量生成模块将这些特征参数按照一定的顺序排列即可生成生物电信号的特征向量，例如 ：Feature Vector = {k1, k2, k3, k4, t1, t2,62, E, Cov}。

[0082] 步骤 205、依据生物电信号的特征参数计算生物电特征向量 ；

[0083] 将生物电信号的特征参数按一定顺序进行排列即可组成生物电的特征向量。

[0084] 步骤 206、将生物电特征向量发送至智能密钥装置 ；

[0085] 步骤 207、智能密钥装置将使用者生物电特征向量与预存的相应的生物电特征向量模板进行匹配比较，依据比较后的结果确定是否匹配。

[0086] 是否匹配是指比较的结果是否超过预先设置的门限值，若超过，则表示该交易者通过身份鉴定。若没有超过，则表示该用户没有通过身份鉴定。智能密钥装置将匹配比较

结果返回主机。

[0087] 本实施例中，匹配比较方法可采用矢量量化方法、隐马尔可夫模型方法、动态时间规整 (DTW) 法或人工神经网络法，上述方法已在音频领域有成熟的应用，其可靠性很高。步骤 208、主机开始访问智能密钥装置中存储的重要数据，智能密钥确认使用者身份合法后，允许主机操作受保护的重要数据。主机对受保护的重要数据进行操作包括读、写、加 / 解密处理等等。

[0088] 本发明也可采用人体电阻、体温、湿度、脉搏等生物特征信号对使用者进行身份鉴定，也可将上述人体生物特征信号与生物电信号进行叠加后，再按实施例所述方法处理成生物电特征向量，与生物电模板信息进行匹配比较，进一步提高对主机使用者身份识别的可靠性和安全性。

[0089] 参阅图 7，为本发明提高智能密钥安全性的装置一实施例示意图，包括生物电检测单元 701、智能密钥单元 702、状态指示单元 703 和电源单元 704。

[0090] 其中，生物电检测单元 701 包括获取单元 7011、信号处理单元 7012、接口单元 7013、接口单元 7014 和存储单元 7014。智能密钥单元 702 包括确认单元 7021、接口单元 7022、接口单元 7023 和存储单元 7024。

[0091] 使用者使用主机预访问智能密钥单元 702 内的重要数据，需在主机上输入个人标识号码，主机通过接口单元 7022 将个人标识号码传送到确认单元 7021，确认单元 7021 在存储单元 7024 中查找是否储存该使用者的生物电向量模板信息，并将查询结果返回主机。存储单元 7024 包括 RAM、FLASH、EEPROM 等存储器。

[0092] 如没有查找到，主机将终止进行后续操作，并向状态指示单元 703 发送一错误信息，状态指示单元 703 显示该信息；如查找到，则通过接口单元 7022 发送获取该使用者生物电信息的指令。

[0093] 接口单元 7022 将该获取使用者生物电信息的指令传送至确认单元 7021，确认单元 7021 通过接口单元 7023、接口单元 7014 将该指令传送至信号处理单元 7012，信号处理单元 7012 通过接口单元 7013 激活获取单元 7011。

[0094] 获取单元 7011 通过专用的仪器获取被使用者生物电信号，生物电信号可以为人体心肌生物电信号、脑电波信号等有较强特征的信号量。生物电信号可通过测量人体两手之间的电位差获取。获取单元 7011 将获取的生物电信号通过接口单元 7013 传送至信号处理单元 7012。

[0095] 信号处理单元 7012 将采集到的生物电信号进行放大、滤波处理，再依据特种电检测方法将生物电波形信号转换为特征参数，如：

[0096] 所述在处理后的生物电信号中提取生物电特征参数包括：

[0097] 计算生物电信号一个波形周期中的斜率；

[0098] 计算生物电信号一个波形周期中峰值时间；

[0099] 计算生物电信号周期波形内采样点值的方差；

[0100] 计算生物电信号周期波形的高阶矩；

[0101] 计算生物电信号周期波形的协方差。

[0102] 所述计算生物电信号一个波形周期中的斜率包括：计算生物电信号中每一个周期内生物电信号的波形从起始点到第一个波峰的上升斜率；从第一个波谷到第二个波峰的上

升斜率；从波峰到最低点的下降斜率；最后一个波峰的上升斜率；

[0103] 所述计算生物电信号一个波形周期中峰值时间包括：计算每一个周期内生物电信号的波形从起点到第一个波峰所用的时间；从第一个波峰到最后一个波峰所用的时间；

[0104] 所述计算生物电信号周期波形内采样点值的方差包括：计算前 n 个周期波形信号内采样点值的方差，并计算出 n 个方差的平均值；

[0105] 所述计算生物电信号周期波形的高阶矩包括：计算前 n 个周期波形信号中每个周期的 4 阶矩，并计算出前 n 个波形信号周期 4 阶矩的平均值。

[0106] 所述计算生物电信号周期波形的协方差包括：计算前 n 个周期波形信号相邻两周期的协方差。其中 n 大于 1。

[0107] 在计算出以上这些特征参数后，只需利用特征向量生成模块将这些特征参数按照一定的顺序排列即可生成生物电信号的特征向量，例如：Feature Vector = {k1, k2, k3, k4, t1, t2, 62, E, Cov}。

[0108] 信号处理单元 7012 并将生物电特征向量通过接口单元 7014 和接口单元 7023 传送至确认单元 7021。信号处理单元 7012 将处理过程中所需数据存储在存储单元 7015 内，存储单元 7015 包括 RAM、FLASH 存储器及外部存储器。

[0109] 确认单元 7021 在存储单元 7024 中调出该使用者的生物电特征向量模板信息，并获取的生物电特征向量与模板信息进行匹配比较。确认单元 7021 预先设置一个门限值，只有当被使用者的生物电特征向量与预先存储的模板信息的匹配超过所述门限值时，确认该被使用者身份；否则该被使用者非法。

[0110] 确认单元 7021 通过接口单元 7022 向主机发送比较结果信息，如该使用者身份被确认，主机开始在存储单元 7024 中读取重要数据，同时，确认单元 7021 允许主机访问存储单元 7024 内的重要数据；如该使用者身份没有被确认，主机向状态指示单元 703 发送身份识别错误信息，状态指示单元 703 显示该信息。

[0111] 电源单元 704 用于为生物电检测单元 701、智能密钥单元 702、状态指示单元 703 提供所需电源。

[0112] 请参阅图 8，为本发明提高智能密钥安全性的装置另一实施例示意图，包括生物电信号采集器 801、存储器 802 和处理器 803。

[0113] 生物电信号采集器用于根据处理器 803 的指令获取主机使用者的生物电信号，并将该信号传送至处理器 803。

[0114] 处理器 803 将生物电信号进行放大、滤波处理，再依据特种电检测方法将处理后的生物电波形信号转换为特征参数，把特征参数按一定顺序进行排列即可组成生物电的特征向量。

[0115] 处理器 803 在存储器 802 中调出该使用者的生物电特征向量模板信息，并获取的生物电特征向量与模板信息进行匹配比较。如果匹配比较结果达到或超过预设的门限值，则确认该使用者身份；如果匹配比较结果没有达到预设的门限值，则认为该使用者非法。

[0116] 处理器 803 将匹配比较结果发送到主机，如果该使用者身份被确定，主机被允许访问存储器 802 内存储的重要数据。

[0117] 存储器 802 包括 RAM、FLASH、EEPROM 存储器及外部存储器，用于存储临时数据、使用者生物电特征向量模板信息及重要工作数据。

[0118] 以上对本发明所提供的一种提高智能密钥安全性的方法及装置，进行了详细介绍，本文中应用了具体个例对本发明的原理及实施方式进行了阐述，以上实施例的说明只是用于帮助理解本发明的方法及其核心思想；同时，对于本领域的一般技术人员，依据本发明的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

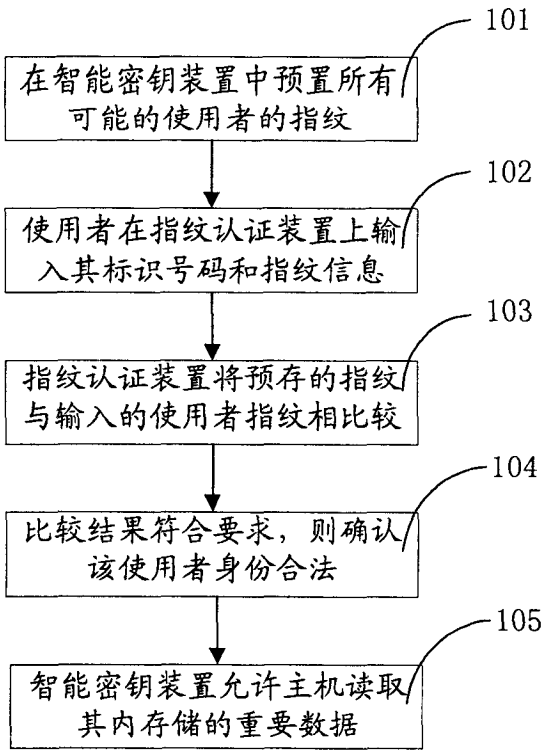

101
在智能密钥装置中预置所有可能的使用者的指纹
102
使用者在指纹认证装置上输入其标识号码和指纹信息
103
指纹认证装置将预存的指纹与输入的使用者指纹相比较
104
比较结果符合要求，则确认该使用者身份合法
105
智能密钥装置允许主机读取其内存储的重要数据

图 1

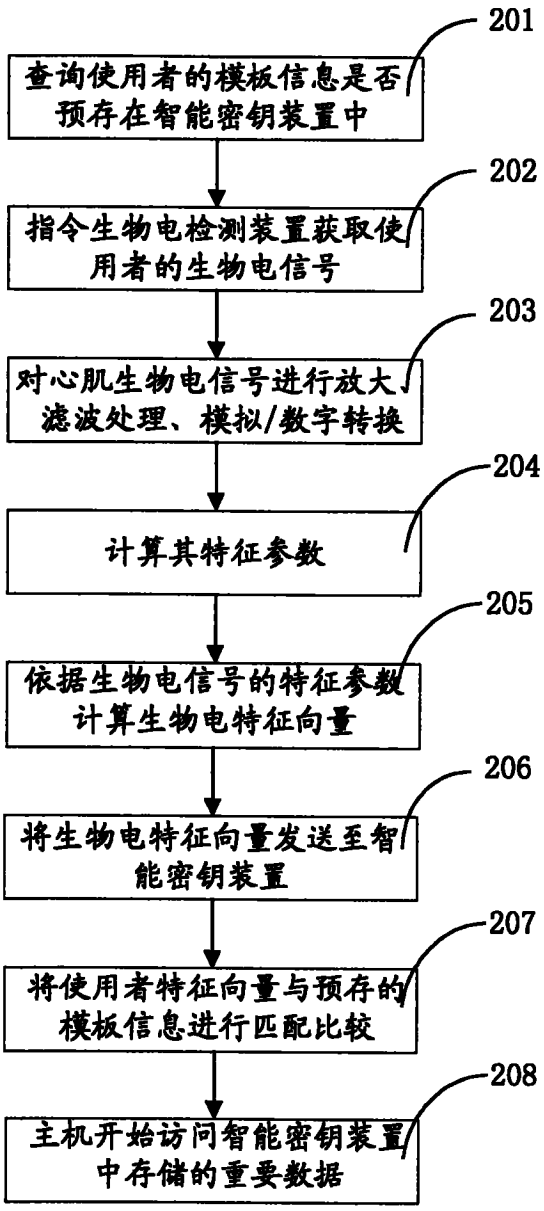

201
查询使用者的模板信息是否预存在智能密钥装置中
202
指令生物电检测装置获取使用者的生物电信号
203
对心肌生物电信号进行放大、滤波处理、模拟/数字转换
204
计算其特征参数
205
依据生物电信号的特征参数计算生物电特征向量
206
将生物电特征向量发送至智能密钥装置
207
将使用者特征向量与预存的模板信息进行匹配比较
208
主机开始访问智能密钥装置中存储的重要数据

图 2

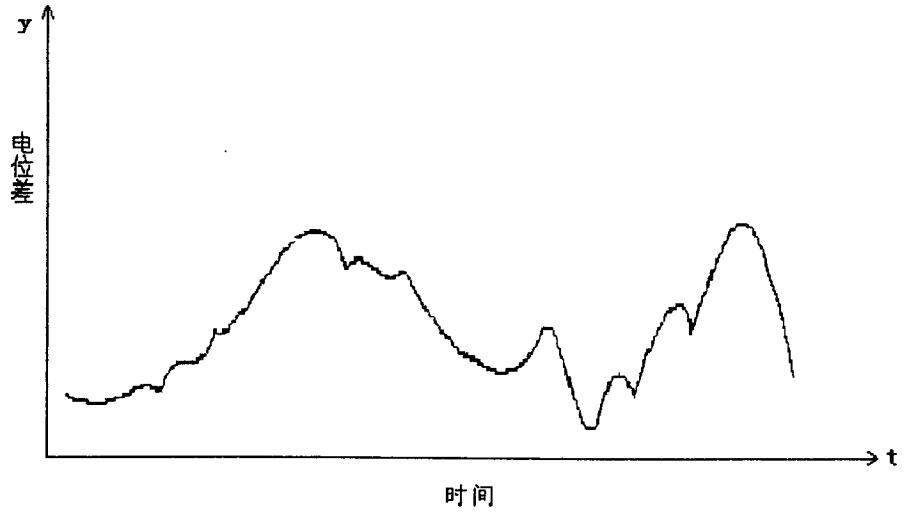


图 3

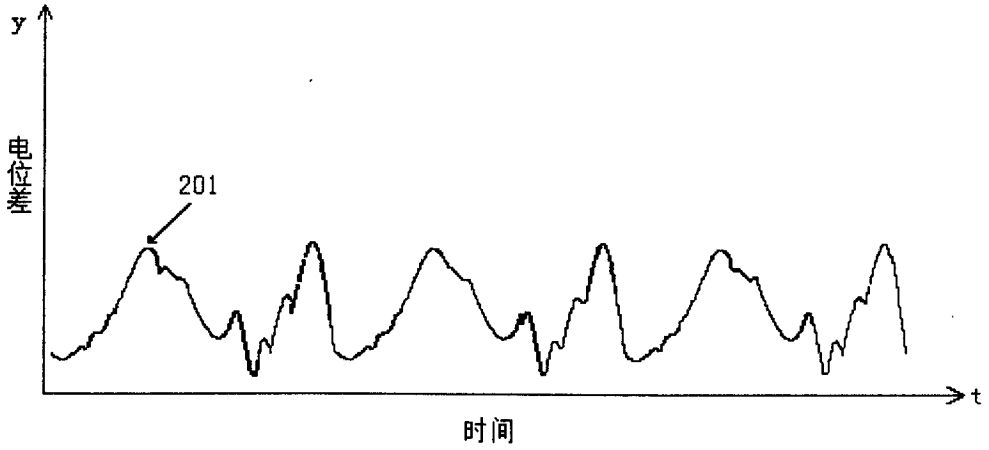


图 4

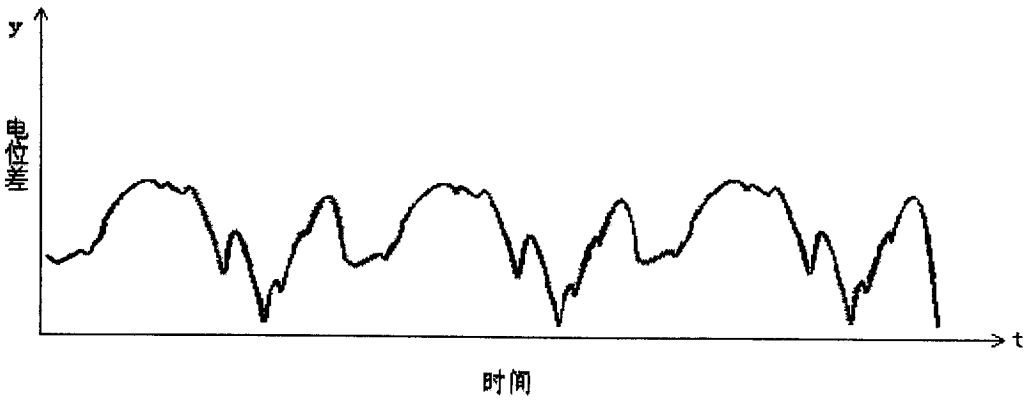


图 5

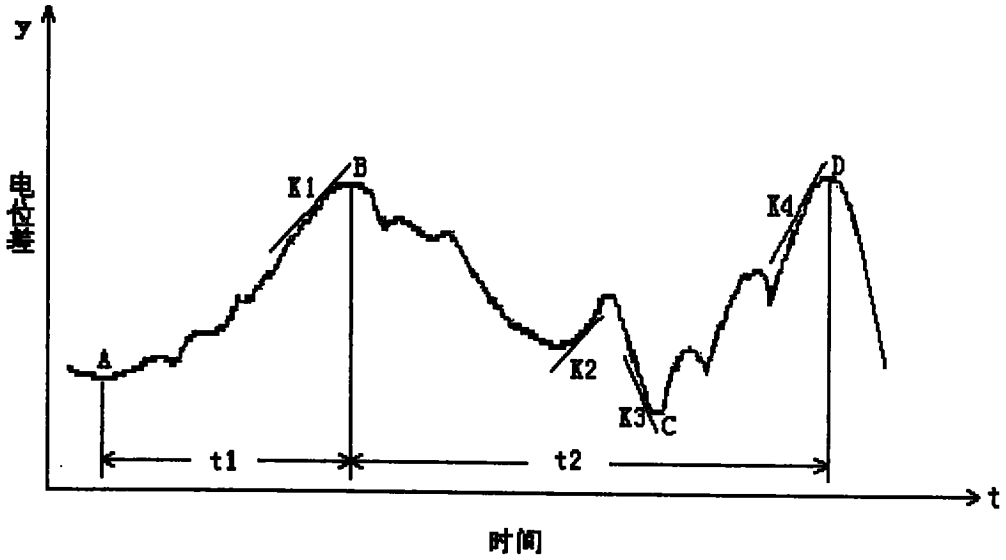

y
电位差
K1
B
K4
D
A
K2
K3
C
t1
t2
t
时间

图 6

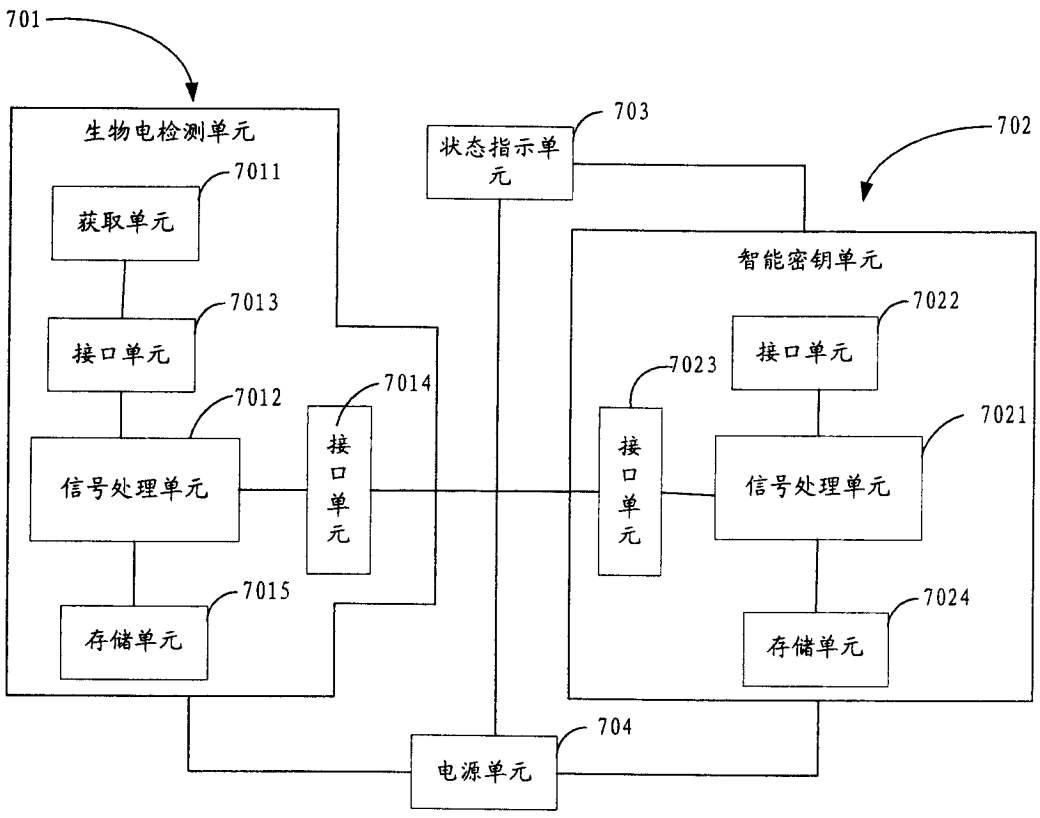

701
生物电检测单元
7011
获取单元
7013
接口单元
7012
信号处理单元
7014
接口单元
7015
存储单元
703
状态指示单元
702
智能密钥单元
7022
接口单元
7023
接口单元
7021
信号处理单元
7024
存储单元
704
电源单元

图 7

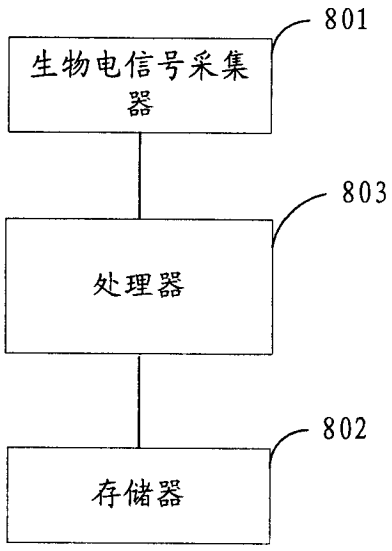


图 8