(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 104993922 B
(45)授权公告日 2018.12.07

(21)申请号 201510273372.6

(22)申请日 2015.05.26

(65)同一申请的已公布的文献号
申请公布号 CN 104993922 A

(43)申请公布日 2015.10.21

(73)专利权人 惠州TCL移动通信有限公司
地址 516006 广东省惠州市仲恺高新区和畅七路西86号

(72)发明人 朱建锋

(74)专利代理机构 深圳市君胜知识产权代理事务所(普通合伙) 44268
代理人 王永文 刘文求

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 27/26(2006.01)
A61B 5/00(2006.01)

(56)对比文件
CN 101773394 A,2010.07.14,
CN 10114767 A,2008.03.26,
CN 104574815 A,2015.04.29,
WO 2015030712 A1,2015.03.05,
CN 1672357 A,2005.09.21,

审查员 王小龙

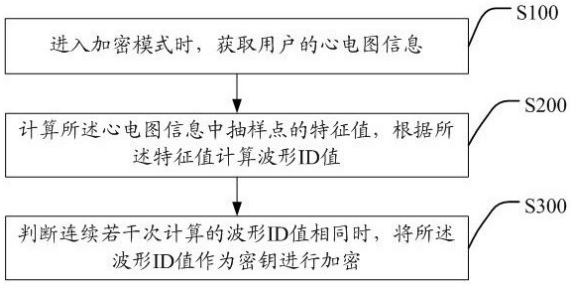
权利要求书2页 说明书6页 附图3页

(54)发明名称

一种智能穿戴设备及其加密、解密方法

(57)摘要

本发明公开了一种智能穿戴设备及其加密、解密方法，加密方法包括：A、进入加密模式时，获取用户的心电图信息；B、计算所述心电图信息中抽样点的特征值，根据所述特征值计算波形ID值；C、判断连续若干次计算的波形ID值相同时，将所述波形ID值作为密钥进行加密；其直接利用现有智能穿戴设备中都设置的心跳探测芯片来获取用户唯一的心电图信息，以心电图中各波段上抽样点的数据进行计算获得波形ID值自动加密；无需用户记录密码且操作方便，不会占用智能穿戴设备的内部空间。



CN 104993922 B

1.一种智能穿戴设备的加密方法,其特征在于,包括:

A、进入加密模式时,获取用户的心电图信息;

B、计算所述心电图信息中抽样点的特征值,根据所述特征值计算波形ID值;

C、判断连续若干次计算的波形ID值相同时,将所述波形ID值作为密钥进行加密;

所述步骤B具体包括:

B1、计算P波、QRS波和T波的最小曲率半径;

B2、计算P波和T波在预设时间内抽样点的个数,在P波和T波上随机分配抽样点并提取;

B3、对P波和T波进行离散傅立叶变换和归一化获得P波、T波的波峰对应的函数;计算QRS波的特征信息量,获得QRS波的波峰对应的函数;

B4、根据P波、T波、QRS波的波峰对应的函数获得波形ID值;

计算QRS波的协方差矩阵,计算协方差矩阵的特征值和特征向量并按从大到小顺序排列,得到特征序列λ_i,i=1,2…L,取M个主要成分得到特征信息量,对特征信息量的数据进行归类,得到相应的数据序列组成加密数据库,该加密数据库即为QRS波的波峰对应的函数;M<L,L为自然数。

2.根据权利要求1所述的智能穿戴设备的加密方法,其特征在于,在所述步骤B2中,所述抽样点的个数等于一个心电图波形的周期乘以抽样频率;

抽样点在P波、QRS波和T波上随机分配,或每隔参考时间分配一抽样点。

3.根据权利要求1所述的智能穿戴设备的加密方法,其特征在于,在所述步骤B3中,对P波和T波进行离散傅立叶变换和归一化获得P波、T波的波峰对应的函数具体包括:

B31、将抽样点组成一个新的波形,进行傅里叶变换后再进行归一化处理;

B32、将归一化后得到的值带入最小曲率半径获得P波、T波的波峰对应的函数。

4.根据权利要求3所述的智能穿戴设备的加密方法,其特征在于,所述步骤B4中,波形ID值为整体归类一个函数$f(ID) \propto \Delta = f(f(H_P), f(H_{QRS}), f(H_T), Ts)$,其中,$f(H_P)$、$f(H_{QRS})$、$f(H_T)$分别为P波、QRS波和T波的波峰对应的函数;Ts为一个心电图波形的周期,Δ为综合环境变化量。

5.一种智能穿戴设备的解密方法,其特征在于,包括:

a、智能穿戴设备开机时检测是否有脉搏跳动:若有执行步骤b;没有则进入待机模式;

b、进入解密模式,采集心电图信息,在心电图波形中提取预设个数的抽样点并计算抽样点的特征值,根据所述特征值计算波形ID值;

c、判断波形ID值是否在密钥容错范围内,是则解密,否则进入待机模式;

计算抽样点的特征值,根据所述特征值计算波形ID值包括:

b1、计算P波、QRS波和T波的最小曲率半径;

b2、计算P波和T波在预设时间内抽样点的个数,在P波和T波上随机分配抽样点并提取;

b3、对P波和T波进行离散傅立叶变换和归一化获得P波、T波的波峰对应的函数;计算QRS波的特征信息量,获得QRS波的波峰对应的函数;

b4、根据P波、T波、QRS波的波峰对应的函数获得波形ID值;

计算QRS波的协方差矩阵,计算协方差矩阵的特征值和特征向量并按从大到小顺序排列,得到特征序列λ_i,i=1,2…L,取M个主要成分得到特征信息量,对特征信息量的数据进行归类,得到相应的数据序列组成加密数据库,该加密数据库即为QRS波的波峰对应的函数;M

<L,L为自然数。

6.根据权利要求5所述的智能穿戴设备的解密方法,其特征在于,在所述步骤c中,所述密钥容错范围是以密钥为基准设置的一个上下波动的范围。

7.一种智能穿戴设备,其特征在于,包括加解密装置,所述加解密装置包括心跳探测芯片和CPU;

所述CPU进入加密模式时,心跳探测芯片获取用户的心电图信息;CPU计算所述心电图信息中抽样点的特征值,根据所述特征值计算波形ID值,判断连续若干次计算的波形ID值相同时,将所述波形ID值作为密钥进行加密并存储;

所述CPU计算所述心电图信息中抽样点的特征值,根据所述特征值计算波形ID值包括:计算P波、QRS波和T波的最小曲率半径;计算P波和T波在预设时间内抽样点的个数,在P波和T波上随机分配抽样点并提取;对P波和T波进行离散傅立叶变换和归一化获得P波、T波的波峰对应的函数;计算QRS波的特征信息量,获得QRS波的波峰对应的函数;

B4、根据P波、T波、QRS波的波峰对应的函数获得波形ID值;

计算QRS波的协方差矩阵,计算协方差矩阵的特征值和特征向量并按从大到小顺序排列,得到特征序列λ_i,i=1,2…L,取M个主要成分得到特征信息量,对特征信息量的数据进行归类,得到相应的数据序列组成加密数据库,该加密数据库即为QRS波的波峰对应的函数;M<L,L为自然数。

8.根据权利要求7所述的智能穿戴设备的加解密装置,其特征在于,所述心跳探测芯片还用于开机时检测是否有脉搏跳动,若有控制CPU进入解密模式,若没有进入待机模式;

解密模式下心跳探测芯片采集心电图信息并传输给CPU,CPU在心电图波形中提取预设个数的抽样点并计算抽样点的特征值,根据所述特征值计算波形ID值,判断波形ID值是否在密钥容错范围内,是则解密,否则进入待机模式。

一种智能穿戴设备及其加密、解密方法

技术领域

[0001] 本发明涉及加密技术领域，特别涉及一种智能穿戴设备及其加密、解密方法。

背景技术

[0002] 随着2015MWC(世界移动通信大会)上面穿戴设备的风靡。越来越多的厂商都投入到了智能手表等智能穿戴设备的研发。智能穿戴设备的发展使新的功能应用也不断被开发。智能穿戴设备的安全保密性为主要研发方向之一。常见的加密方式如密码加密、指纹加密等。由于智能穿戴设备的体积相对较小，密码加密需用户牢记密码且输入不方便；若增加指纹识别模组来进行指纹加密，或采用其他身份识别的模组则会占用一定的空间、从而使智能穿戴设备的结构可塑性变的更小。

[0003] 因而现有技术还有待改进和提高。

发明内容

[0004] 本发明的目的在于提供一种智能穿戴设备及其加密、解密方法，以解决现有智能穿戴设备加密操作不方便、占用空间的问题。

[0005] 为了达到上述目的，本发明采取了以下技术方案：

[0006] 一种智能穿戴设备的加密方法，其包括：

[0007] A、进入加密模式时，获取用户的心电图信息；

[0008] B、计算所述心电图信息中抽样点的特征值，根据所述特征值计算波形ID值；

[0009] C、判断连续若干次计算的波形ID值相同时，将所述波形ID值作为密钥进行加密。

[0010] 所述的智能穿戴设备的加密方法中，所述步骤A具体包括：

[0011] A1、计算P波、QRS波和T波的最小曲率半径；

[0012] A2、计算P波和T波在预设时间内抽样点的个数，在P波和T波上随机分配抽样点并提取；

[0013] A3、对P波和T波进行离散傅立叶变换和归一化获得P波、T波的波峰对应的函数；计算QRS波的特征信息量，获得QRS波的波峰对应的函数；

[0014] A4、根据P波、T波、QRS波的波峰对应的函数获得波形ID值。

[0015] 所述的智能穿戴设备的加密方法中，在所述步骤A2中，所述抽样点的个数等于一个心电图波形的周期乘以抽样频率；

[0016] 抽样点在P波、QRS波和T波上随机分配，或每隔参考时间分配一抽样点。

[0017] 所述的智能穿戴设备的加密方法中，在所述步骤A3中，对P波和T波进行离散傅立叶变换和归一化获得P波、T波的波峰对应的函数具体包括：

[0018] A31、将抽样点组成一个新的波形，进行傅里叶变换后再进行归一化处理；

[0019] A32、将归一化后得到的值带入最小曲率半径获得P波、T波的波峰对应的函数。

[0020] 所述的智能穿戴设备的加密方法中，所述步骤A4中，波形ID值为$f(ID) \propto \Delta = f(f(H_P), f(H_{QRS}), f(H_T), T_S)$，其中，$f(H_P)$、$f(H_{QRS})$、$f(H_T)$分别为P波、QRS波和T波的波峰对应

的函数;Ts为一个心电图波形的周期,Δ为综合环境变化量。

[0021] 一种智能穿戴设备的解密方法,其包括:

[0022] a、智能穿戴设备开机时检测是否有脉搏跳动:若有执行步骤b;没有则进入待机模式;

[0023] b、进入解密模式,采集心电图信息,在心电图波形中提取预设个数的抽样点并计算抽样点的特征值,根据所述特征值计算波形ID值;

[0024] c、判断波形ID值是否在密钥容错范围内,是则解密,否则进入待机模式。

[0025] 所述的智能穿戴设备的解密方法中,在所述步骤c中,所述密钥容错范围是以密钥为基准设置的一个上下波动的范围。

[0026] 一种智能穿戴设备,其包括加解密装置,所述加解密装置包括心跳探测芯片和CPU;

[0027] 所述CPU进入加密模式时,心跳探测芯片获取用户的心电图信息;CPU计算所述心电图信息中抽样点的特征值,根据所述特征值计算波形ID值,判断连续若干次计算的波形ID值相同时,将所述波形ID值作为密钥进行加密并存储。

[0028] 所述的智能穿戴设备的加解密装置中,所述心跳探测芯片还用于开机时检测是否有脉搏跳动,若有控制CPU进入解密模式,若没有进入待机模式;

[0029] 解密模式下心跳探测芯片采集心电图信息并传输给CPU,CPU在心电图波形中提取预设个数的抽样点并计算抽样点的特征值,根据所述特征值计算波形ID值,判断波形ID值是否在密钥容错范围内,是则解密,否则进入待机模式。

[0030] 相较于现有技术,本发明提供的智能穿戴设备及其加密、解密方法,进入加密模式时,获取用户的心电图信息;计算所述心电图信息中抽样点的特征值,根据所述特征值计算波形ID值;判断连续若干次计算的波形ID值相同时,将所述波形ID值作为密钥进行加密;其直接利用现有智能穿戴设备中都设置的心跳探测芯片来获取用户唯一的心电图信息,以心电图中各波段上抽样点的数据进行计算获得波形ID值自动加密;无需用户记录密码且操作方便,不会占用智能穿戴设备的内部空间。

附图说明

[0031] 图1为现有心电图波形的示意图。

[0032] 图2为本发明提供的智能穿戴设备的加密方法的方法流程图。

[0033] 图3为本发明提供的智能穿戴设备的加密方法中一个心电图波形的周期示意图。

[0034] 图4为本发明提供的智能穿戴设备的加密方法中曲率半径的示意图。

[0035] 图5为本发明提供的智能穿戴设备的解密方法的方法流程图。

[0036] 图6为本发明提供的智能穿戴设备的加解密装置的结构框图。

具体实施方式

[0037] 心肌细胞膜是半透膜,静息状态时,膜外排列一定数量带正电荷的阳离子,膜内排列相同数量带负电荷的阴离子,膜外电位高于膜内,称为极化状态。静息状态下,由于心脏各部位心肌细胞都处于极化状态,没有电位图的等电位线。心肌细胞在受到一定强度的刺激时,细胞膜通透性发生改变,大量阳离子短时间内涌入膜内,使膜内电位由负变正,这个

过程称为除极。对整体心脏来说，心肌细胞从心内膜向心外膜顺序除极过程中的电位变化，由电流记录仪描记的电位曲线称为除极波，即体表心电图上心房的P波和心室的QRS波。细胞除极完成后，细胞膜又排出大量阳离子，使膜内电位由正变负，恢复到原来的极化状态，此过程由心外膜向心内膜进行，称为复极。同样心肌细胞复极过程中的电位变化，由电流记录仪描记出称为复极波。由于复极过程相对缓慢，复极波较除极波低。心房的复极波低、且埋于心室的除极波中，体表心电图不易辨认。心室的复极波在体表心电图上表现为T波。整个心肌细胞全部复极后，再次恢复极化状态，各部位心肌细胞间没有电位差，体表心电图记录到等电位线。因此，每一个波段代表心脏的不同部位。图1中示出窦房结、房室结(房结区、结区、结希区)、希氏束、束支、心室复极对应的波段，各波段组合为一个周期的心电图波形其为现有技术，此处不作详述。

[0038] 基于上述的心电图波形，本发明提供一种智能穿戴设备及其加密、解密方法，利用现有的智能穿戴设备中都设置的心跳探测芯片来获取用户唯一的心电图信息。以心电图中各波段上抽样点的数据作为身份的识别标识，进行自动地加密和解密；无需用户记录密码且操作方便，不会占用智能穿戴设备的内部空间。为使本发明的目的、技术方案及效果更加清楚、明确，以下参照附图并举实施例对本发明进一步详细说明。应当理解，此处所描述的具体实施例仅用以解释本发明，并不用于限定本发明。

[0039] 请参阅图2，其为本发明提供的智能穿戴设备的加密方法流程图。本发明提供的加密方法包括：

[0040] S100、进入加密模式时，获取用户的心电图信息；

[0041] S200、计算所述心电图信息中抽样点的特征值，根据所述特征值计算波形ID值；

[0042] S300、判断连续若干次计算的波形ID值相同时，将所述波形ID值作为密钥进行加密。

[0043] 由于每个人的心脏结构不完全一样，科学界已经证实所有人的心电图波形不可能完全一样。随着环境的变化、以及心脏本身受到疾病直接或者间接的影响，整个心电图波形的相关变量也会变化。通过特征值提取后能获得每个人自己特有的波形ID值。

[0044] 本实施例根据上述结论，采用用户的心电图信息作为加密的密钥。需要获取密钥时，用户带上智能穿戴设备后点击屏幕中的加密图标或加密选项，即可进入加密模式。在加密模式下，智能穿戴设备的心跳探测芯片采集用户的心电图信息，进行相应计算、判断获得波形ID值作为密钥进行加密。加密成功后提示用户，并自动退出加密模式，使智能穿戴设备能正常工作。

[0045] 如图3所示，心电图信息包括多个心电图波形、波形上所有点的坐标值、一个心电图波形的周期、抽样频率。心脏跳一次出现一个周期为T s的波形。在所述步骤S200中，所述特征值的计算包括计算P波和T波的曲率半径来获得其波峰值，以及计算QRS波的特征信息向量来获得其波峰值。假设P波，QRS波及T波的波峰对应的函数分别为f(HP)，f(HQRS)，f(HT)，则波形ID值的密码模型为$f(ID) \propto \Delta = f(f(HP), f(HQRS), f(HT), Ts)$。(Δ综合环境变化量)。

[0046] 所述步骤S200具体包括：

[0047] 步骤201、计算P波、QRS波和T波的最小曲率半径。

[0048] 从图3可知P波和T波是一种正弦波，根据P波和T波这一特征计算其波峰及其波峰

趋势，可采用计算P波和T波的曲率半径来转化为波峰特征点的采集。在图4中根据波形上的点x、y、z的值找到最小曲率半径，计算公式为 $\delta = \frac{\left|\vec{a} - \vec{c}\right|}{\left|\vec{a}\right|}$ 。当δ最大时曲率半径就最小。根据δ的值可获得P波和T波的上升斜率。QRS波为三角波，也采用最小曲率半径计算获得其上升斜率趋势。

[0049] 接着根据该最小曲率半径的公式，进行傅立叶特征系数和归一化转换。即步骤202、计算P波和T波在预设时间内抽样点的个数，在P波和T波上随机分配抽样点并提取。

[0050] 以P波为例，预设时间为一分钟。假设人的标准心律为80次每分钟，则一个心电图波形(即图3中的一个周期Ts)的周期为0.75秒(60s/80次)，一分钟内有80个周期。如果抽样频率是8000Hz，那么一个心律为80次的心电图周期就含有6000(0.75s×8000Hz)个抽样点，此为标准心律的抽样点Nn。

[0051] 在P波上可随机分配6000个抽样点，或采用每隔参考时间(如0.01s、或0.005s)设置一抽样点进行分配。如果心跳次数变化则抽样点也会相应变化，如有的人每分钟跳74次或88次，则一个心电图波形的周期对应变为约0.81s或0.68s，对应地抽样点为6480个或5440个，总会在6000个抽样点这一标准值的上下变化。

[0052] S203、对P波和T波进行离散傅立叶变换和归一化。

[0053] 本步骤中，首先要计算P波和T波的抽样点的特征值。以P波为例，特征值的计算是先将其抽样点组成一个新的波形，即进行傅里叶变换，以了解这些抽样点的变化趋势。

[0054] 假设获取的整体的心电图波形h(n)(即一分钟内80个周期)的长度为N，其离散傅里叶变换为：$H(k) = \sum_{n=0}^{N-1} h(n) e^{-j2\pi kn/N}$ 。其中，0<=k<=N-1。由于实际的N可能比Nn(Nn=6000)大也可能小，则定义心电图波形的长度比α=N/Nn，如果α>1，则记录心律高于标准心律，如果α<1则低于标准心律。傅里叶变换可使P波和T波的数据趋向更加稳定化。

[0055] 接着需对抽样点的值进行归一化，保留值相近的抽样点，滤除差距较大的抽样点。若将抽样点数固定为Nn(6000)，需设置一个标量Tn，Tn=Ts/α，Ts=1/fs。由此可得归一化的周期信号函数：

[0056] $h(n) = \sum_{k=0}^{M} \left|H(k)\right| \cos\left(2\pi k \frac{f_s}{N} n T_n + \angle H(k)\right)$ ，其中，M为心电图频谱最高整数频率，一般为[0,100]Hz；fs为脉搏的跳动频率。

[0057] 根据公式 $\delta = \frac{\left|\vec{a} - \vec{c}\right|}{\left|\vec{a}\right|}$ ，把得到的h(n)的值相应的填充到x、y、z相对应的坐标值。横坐标为采集时间所对应的数值，可以直接用N表示。纵坐标为纵向采集的电压转换的数

值，经由傅立叶变换及归一化剔除其中跳动的离散值。其中$\overrightarrow{\mathbf{a}}$为z的坐标减去x坐标，$\overrightarrow{\mathbf{c}}$为y的坐标减去x的坐标。

[0058] 找到最小曲率半径也就找到波峰值。同时也能根据向量的变化得到波的曲率变化也就是波的变化趋势。把所有得到的数据和变化趋势形成相应的加密数据库进行储存。T波的波峰函数的计算方式与P波相同，此处不作赘述。加密数据库即为P波、T波的波峰对应的函数$f(H_P)$，$f(H_T)$。

[0059] 接着计算QRS波的特征信息量来获得QRS波的波峰对应的函数；

[0060] 由于QRS波与P波和T波不同，其计算方式也不相同。假设采集Z段个心跳波段$Z=\{Z_i\}$，包含有C类，其中每个类中共包含C_i个波段集，总共含有$N=\sum_{i=1}^{C}C_i$个波段。一个波段假设为z_{ij}。所有的波段都以QSR波的波峰为基点，长度为L，小于L的以0补齐，则QRS波的协方差矩阵为$S=\frac{1}{L}\sum_{i=1}^{C}\sum_{j=1}^{C_i}(Z_{ij}-\bar{Z})(Z_{ij}-\bar{Z})^r$，S为N×N的方阵，$\bar{Z}=\frac{1}{L}\sum_{i=1}^{C}\sum_{j=1}^{C_i}Z_{ij}$为平均波段集。计算S的特征值和特征向量并按从大到小顺序排列，得到特征序列λ_i，i=1，2…L，为了计算方便取M个主要成分M<L，得到特征信息量η，$\eta=\sum_{i=1}^{M}\lambda_i/\sum_{i=1}^{L}\lambda_i$，对η的数据进行归类，得到相应的数据序列组成加密数据库，该加密数据库即为QRS波的波峰对应的函数$f(H_{QRS})$。

[0061] 步骤204、、根据P波、T波、QRS波的波峰对应的函数获得波形ID值。

[0062] 综上所述，整体归类一个函数$f(ID)\propto\Delta=f(f(H_P),f(H_{QRS}),f(H_T),Ts)$。（Δ为综合环境变化量）。f(ID)即为波形ID值。

[0063] 由于人体的脉搏跳动是以1Hz为单位的，基于环境或生理因素对心电图采集的干扰，需要一定量的样本信息进行组合。为了更加准确地分析定量，最好连续采集2分钟以上为宜。若上述计算过程每分钟执行一次，则判断连续3次获得的波形ID值相同，则将该波形ID值作为密钥进行加密，并将该波形ID值储存到指定的Flash（可擦写掉电保护存储器）中。基于人体处于不同活动状态、或生理状态下，心跳不同，考虑这些因素的影响。因此，所述步骤S300中，连续若干次计算的波形ID值相同指的是若干次的波形ID值都在预设范围即判断相同。

[0064] 需要理解的是，由于特征值的计算与抽样点有关，而抽样点是随机分配的。则每次加密时获得的密钥不同，这样大大增加了密钥破译的难度，保护了用户的隐私。

[0065] 请参阅图5，基于上述的智能穿戴设备的加密方法，本发明还相应提供一种智能穿戴设备的解密方法，其包括：

[0066] S10、智能穿戴设备开机时检测是否有脉搏跳动，若有进入解密模式，没有则进入待机模式；

[0067] S20、采集心电图信息，在心电图波形中提取预设个数的抽样点并计算抽样点的特征值，根据所述特征值计算波形ID值；

[0068] S30、判断波形ID值是否在密钥容错范围内，是则解密，否则保持待机模式。

[0069] 当智能穿戴设备开机时，心跳探测芯片先探测是否有脉搏跳动，如没有停止探测，表示用户没有带上智能穿戴设备，此时可进入待机模式，也可以自动关闭智能穿戴设备。所述待机模式表示该智能穿戴设备没有解密不能工作。在该待机模式下，只要探测到脉搏跳动(如开机后用户才带上智能穿戴设备)就可进入解密模式。

[0070] 在所述步骤S20中，可先采集一个周期(如图3中一个Ts周期的波形)的心电图波形。基于6000个抽样点已经通过矩阵变化，整理进行归类，所以实际比较的数据已经集中在某个区域。采集6000个点是为了能够全面的分析相对的数据，在实际的密钥对比的过程中会适当降低抽样点的量，加快对比速度。在一个周期中，可提取预设个数(1000个)的抽样点，根据加密时的计算过程计算出这些抽样点的特征值，从而获得P波、QRS波、T波的特征信息量。即可获得最终的波形ID值。

[0071] 将MCU处理得到的波形ID值和Flash存储的比较，如果当前计算的波形ID值在密钥容错范围内，则表示解密成功，智能穿戴设备进入正常工作状态。如不在密钥容错范围内，继续对下一个周期的心电图波形进行抽样点提取和特征值、特征信息量的计算判断。若连接判断预设周期(如10个周期)的心电图波形都无法匹配，则提示解密失败，可保持待机模式或直接关机。

[0072] 基于环境因素和生理的影响，用户的心电图波形会有一定的不同。本实施例设置密钥容错范围，即计算的波形ID值与密钥比对的过程中进行相对的容错机制，以密钥为基准设置一个上下波动的范围，只要计算的波形ID值在这个范围内，可认为计算的波形ID值与密钥相等。

[0073] 请一并参阅图6，基于上述的智能穿戴设备的加密方法，本发明还相应提供一种加解密装置，包括心跳探测芯片1和CPU 2；

[0074] 所述CPU 2进入加密模式时，心跳探测芯片获取用户的心电图信息；CPU计算所述心电图信息中抽样点的特征值，根据所述特征值计算波形ID值，判断连续若干次计算的波形ID值相同时，将所述波形ID值作为密钥进行加密并存储。

[0075] 所述心跳探测芯片还用于开机时检测是否有脉搏跳动，若有控制CPU进入解密模式，若没有进入待机模式；

[0076] 解密模式下心跳探测芯片采集心电图信息并传输给CPU，CPU在心电图波形中提取预设个数的抽样点并计算抽样点的特征值，根据所述特征值计算波形ID值，判断波形ID值是否在密钥容错范围内，是则解密，否则进入待机模式。

[0077] 综上所述，本发明利用现有的智能穿戴设备中都设置的心跳探测芯片来获取用户唯一的心电图信息，以心电图中各波段上抽样点的数据进行相关计算获得波形ID值，以该波形ID值为密钥进行自动地加密和解密；无需用户记录密码且操作方便，不会占用智能穿戴设备的内部空间。

[0078] 可以理解的是，对本领域普通技术人员来说，可以根据本发明的技术方案及其发明构思加以等同替换或改变，而所有这些改变或替换都应属于本发明所附的权利要求的保护范围。

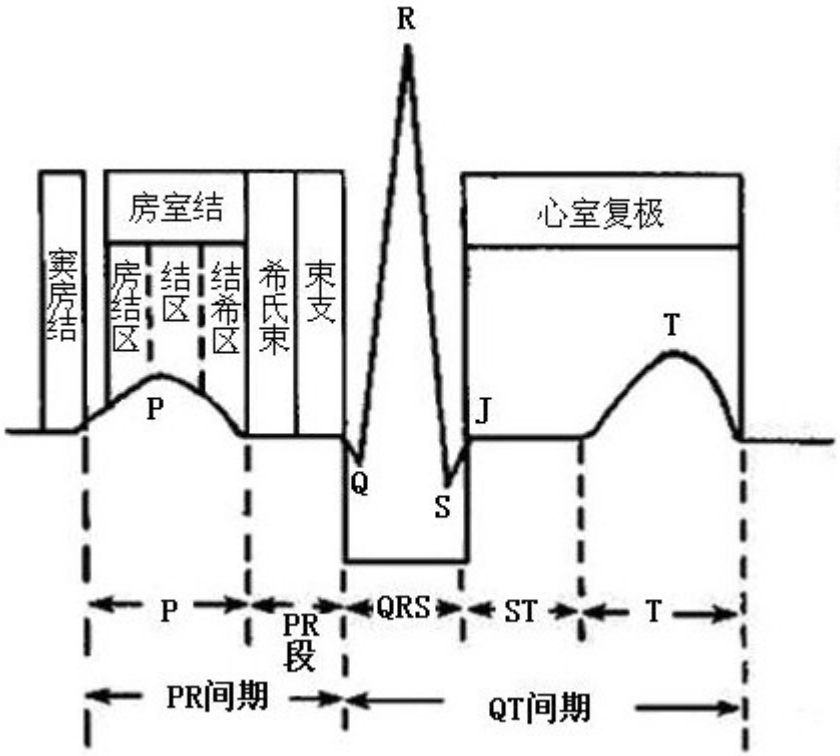

R
房室结
心室复极
窦房结
房结区
结区
结希区
希氏束
束支
T
P
J
Q
S
P
QRS
ST
T
PR段
PR间期
QT间期

图1

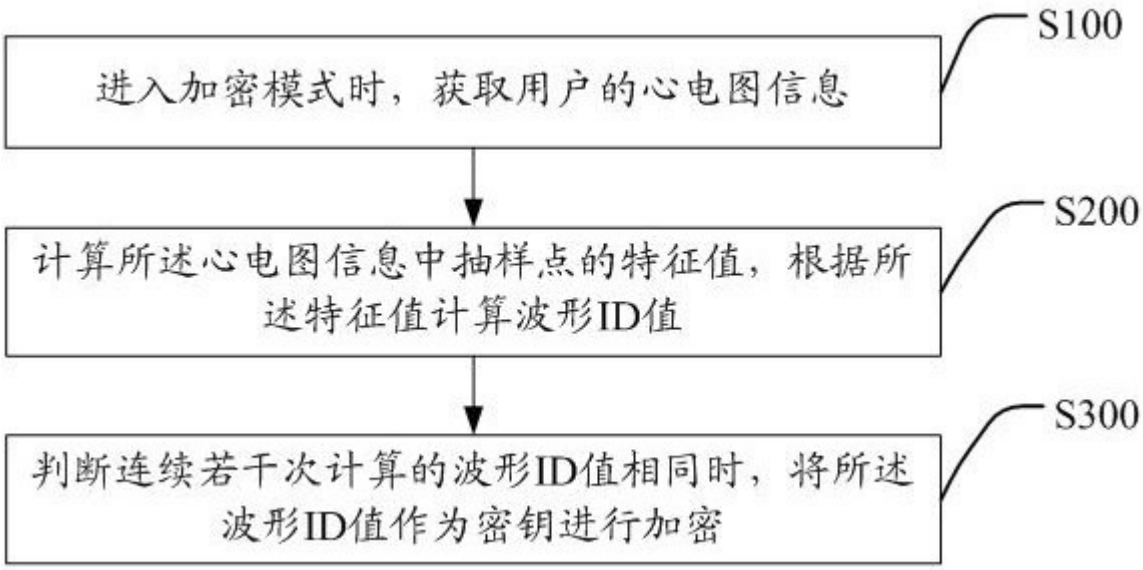

S100
进入加密模式时，获取用户的心电图信息
S200
计算所述心电图信息中抽样点的特征值，根据所述特征值计算波形ID值
S300
判断连续若干次计算的波形ID值相同时，将所述波形ID值作为密钥进行加密

图2

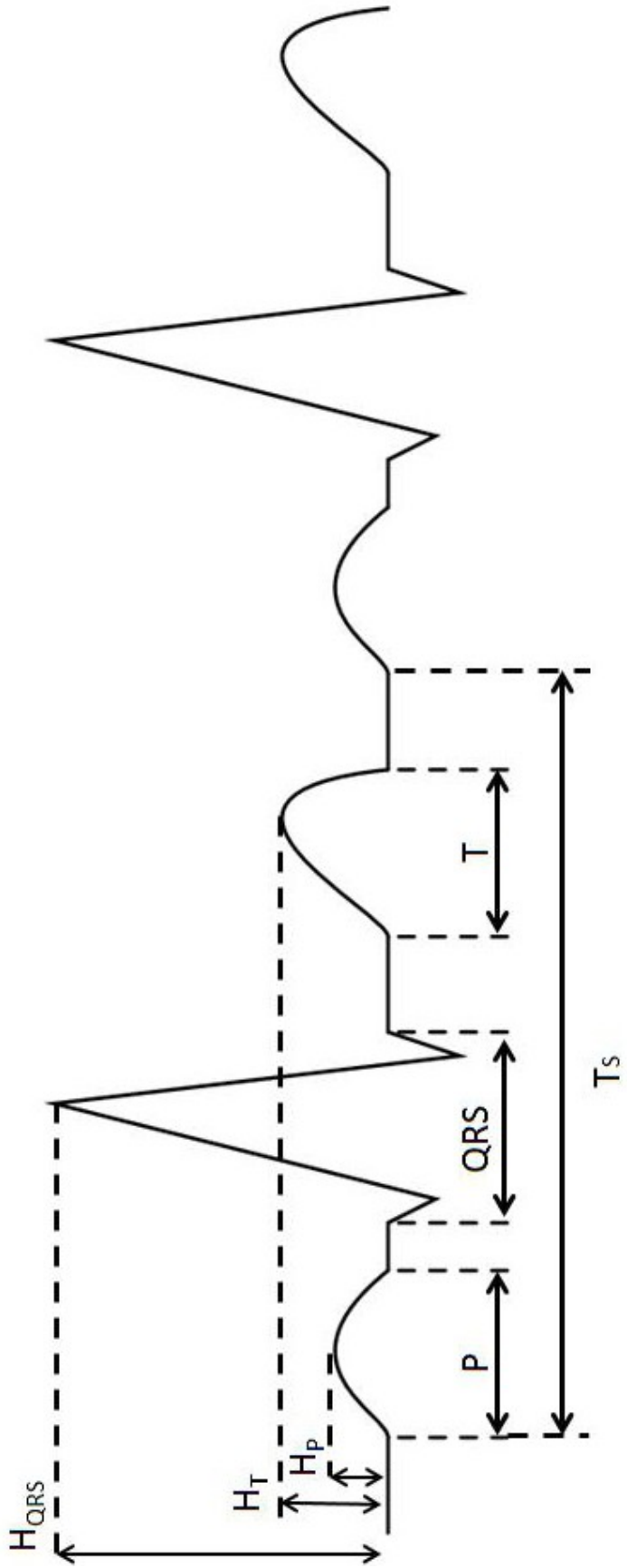


图3

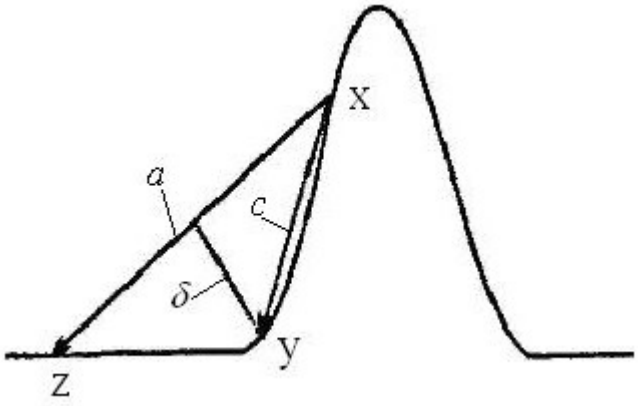

x
a
c
δ
y
z

图4

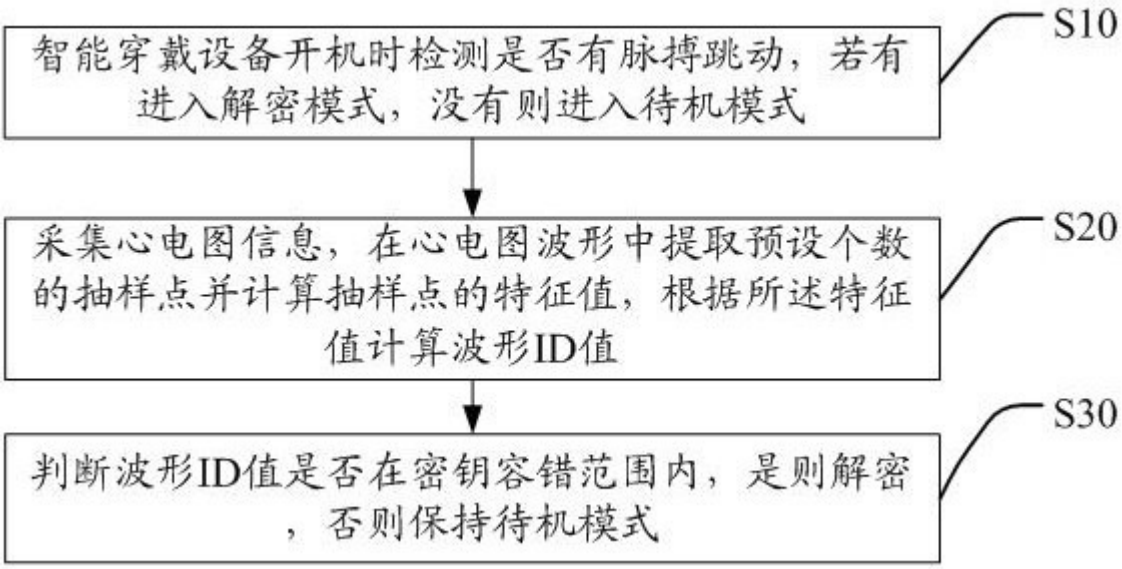

智能穿戴设备开机时检测是否有脉搏跳动，若有进入解密模式，没有则进入待机模式
S10
采集心电图信息，在心电图波形中提取预设个数的抽样点并计算抽样点的特征值，根据所述特征值计算波形ID值
S20
判断波形ID值是否在密钥容错范围内，是则解密，否则保持待机模式
S30

图5

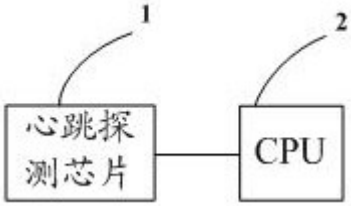

1
2
心跳探测芯片
CPU

图6

专利名称(译)	一种智能穿戴设备及其加密、解密方法		
公开(公告)号	CN104993922B	公开(公告)日	2018-12-07
申请号	CN201510273372.6	申请日	2015-05-26
[标]申请(专利权)人(译)	惠州TCL移动通信有限公司		
申请(专利权)人(译)	惠州TCL移动通信有限公司		
当前申请(专利权)人(译)	惠州TCL移动通信有限公司		
[标]发明人	朱建锋		
发明人	朱建锋		
IPC分类号	H04L9/00 H04L27/26 A61B5/00		
代理人(译)	王永文		
审查员(译)	王小龙		
其他公开文献	CN104993922A		
外部链接	Espacenet SIPO		

摘要(译)

本发明公开了一种智能穿戴设备及其加密、解密方法，加密方法包括：A、进入加密模式时，获取用户的心电图信息；B、计算所述心电图信息中抽样点的特征值，根据所述特征值计算波形ID值；C、判断连续若干次计算的波形ID值相同时，将所述波形ID值作为密钥进行加密；其直接利用现有智能穿戴设备中都设置的心跳探测芯片来获取用户唯一的心电图信息，以心电图中各波段上抽样点的数据进行计算获得波形ID值自动加密；无需用户记录密码且操作方便，不会占用智能穿戴设备的内部空间。