(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 110598424 A
(43)申请公布日 2019.12.20

(21)申请号 201910726569.9

(22)申请日 2019.08.07

(71)申请人 王满
地址 北京市门头沟区石门营新区五区6号楼2单元602
申请人 王江源

(72)发明人 王江源 王满

(74)专利代理机构 昆明知道专利事务所(特殊普通合伙企业) 53116
代理人 姜开侠 姜开远

(51)Int.Cl.
G06F 21/60(2013.01)
G06F 21/62(2013.01)
A61B 5/00(2006.01)
A61B 5/024(2006.01)
A61B 5/029(2006.01)
A61B 5/11(2006.01)

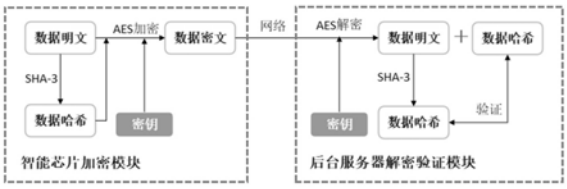
权利要求书2页 说明书5页 附图2页

(54)发明名称

一种基于心脏功能动态监测与分析的数据加密—解密系统及方法

(57)摘要

本发明公开了一种基于心脏功能动态监测与分析的数据加密-解密系统及方法,包括特征ID装置、逻辑电路加密装置、识别解密装置,所述解密装置用于接受密文和心脏智能贴片ID后,通过数据库查找出ID对应的密钥,进行解密。本发明采用便携式智能可穿戴设备对心脏机械振动进行体外监测,实时非侵入地获取心脏的振动信息,结合数字处理、机器学习和人工智能技术模式识别和智能诊断,早期发现心脏物理结构和搏动节律异常,如瓣膜病变、心脏壁的运动异常、心脏射血分数改变、心律失常等。结合预警报告系统,实现心脏疾病早预警与及时医护的目的。对严重心律失常、心绞痛、急性心肌梗死的早期预警监测,对照手术后康复监测,居家养老人群,体育运动人群的日常监护意义重大。



CN 110598424 A

1.一种基于心脏功能动态监测与分析的数据加密-解密系统,其特征在于,所述数据加密-解密系统中的加密装置固化于心脏智能贴片中,识别解密装置位于后台服务器或智能终端设备,具体包括,

所述特征ID装置,用于针对心脏智能贴片产生一个ID和256位的密钥对,标识一个心脏智能贴片,作为其唯一身份识别密钥,固化于心脏智能贴片中,同时存入后台数据库;

所述逻辑电路加密装置,用于对原始数据执行SHA(安全散列算法)哈希算法,得到哈希值,附加在原始数据的末端形成明文,然后使用密钥对明文进行AES加密,得到密文,密文连同设备ID一起传输;

所述识别解密装置,用于接受密文和心脏智能贴片ID后,通过数据库查找出ID对应的密钥,进行解密,从解密数据中分离出明文和哈希值,再次对明文进行同样的哈希算法,将计算得到哈希值与解密得到的哈希值进行对比,如果完全一致,则接受数据。

2.根据权利要求1所述基于心脏功能动态监测与分析的数据加密-解密系统,其特征在于,还包括所述识别接收装置,用于解密的数据再次哈希算法,校验哈希值,如果匹配,则接收数据;如果不匹配,说明数据可能被篡改,则拒绝接收,丢弃数据。

3.根据权利要求1所述基于心脏功能动态监测与分析的数据加密-解密系统,其特征在于,还包括密文暂存装置,用于加密后的密文(即预警信息)的暂时存储,位于芯片存储器之闪存中。

4.根据权利要求1所述基于心脏功能动态监测与分析的数据加密-解密系统,其特征在于,还包括预警启动装置,用于根据密文“携带预警事件信息”启动预警机制,并提示相应预警级别;同时移动智能终端的液晶显示屏显示文字和图标提示预警信息与级别。

5.根据权利要求4所述基于心脏功能动态监测与分析的数据加密-解密系统,其特征在于,所述预警启动装置根据预警级别不同,显示预警状态:轻微预警时,黄灯闪烁;中等级别预警时,红灯闪烁;危急预警时,同时出现红灯闪烁和蜂鸣器响应。

6.一种基于心脏功能动态监测与分析的数据加密-解密方法,其特征在于,具体包括下列步骤,

(1)通过所述特征ID装置标识生产一个ID和256位的密钥对,标识一个心脏智能贴片,作为其唯一身份识别密钥,存入数据库;

(2)通过所述逻辑电路加密装置对原始数据执行SHA(安全哈希算法)哈希算法,得到哈希值,附加在原始数据的末端形成明文,然后使用密钥对明文进行AES(高级加密算法)加密,得到密文,密文连同设备ID一起传输;

(3)通过所述识别解密装置,用于接受密文和心脏智能贴片ID后,通过数据库查找出ID对应的密钥,进行解密。

7.根据权利要求6所述基于心脏功能动态监测与分析的数据加密-解密方法,其特征在于,还通过所述识别接收装置,将解密的数据再次执行哈希算法,校验哈希值,如果匹配,则接收数据;如果不匹配,说明数据可能被篡改,则拒绝接收,丢弃数据。

8.根据权利要求6所述基于心脏功能动态监测与分析的数据加密-解密方法,其特征在于,还通过密文暂存装置将加密后的密文(即预警信息)暂时存储于芯片存储器之闪存中。

9.根据权利要求6所述基于心脏功能动态监测与分析的数据加密-解密系统,其特征在于,还通过预警启动装置根据密文“携带预警事件信息”启动预警机制,并提示相应预警级

别;并通过移动智能终端的液晶显示屏显示文字和图标提示预警信息与级别。

10.根据权利要求9所述基于心脏功能动态监测与分析的数据加密-解密方法,其特征在于,通过所述预警启动装置启动预警机制,并根据预警级别不同作出不同的预警提示:轻微预警时,黄灯闪烁;中等级别预警时,红灯闪烁;危急预警时同时出现红灯闪烁并发出蜂鸣。

一种基于心脏功能动态监测与分析的数据加密—解密系统及方法

技术领域

[0001] 本发明属于智能医疗器械技术领域，具体涉及一种基于心脏功能动态监测与分析的数据加密-解密系统及方法。

背景技术

[0002] 心脏疾病是人类第一号杀手，今天全球有数以十亿计的心脏病患者，需要得到及时、适当和成本可负担的医疗护理。传统的心电图(ECG)只能发现心电信号异常，对心脏物理结构本身的缺损、病变、老化、功能丧失(如心肌部分坏死)却作用不大或无能为力。超声心动图、计算机断层扫描(CT)、磁共振成像(MRI)及心肌灌注核素扫描等检测手段需要大型设备和专业人员操作，检测成本高，且难以做到随时随地监测，失去宝贵的病理信息和抢救机会。

[0003] 近年来，随着微机电系统(MEMS)技术的发展和人群健康需求的提高，针对心脏健康监测的便携式可穿戴设备成为了热门研究领域。但大部分研究和产品基于传统的ECG，Pranav Rajpurkar报道过，对来自可穿戴设备的数万份单导联ECG进行了分析，使用一个34层的卷积神经网络(CNN)，对心律失常的诊断能力可以达到人类医学专家的水平。但由于ECG技术本身的局限性，并不能及时、完整地反映心脏的健康状态，所以研究人员很早就注意到体外心脏振动信号能反映出心脏的结构和功能变化，以弥补ECG的不足，试图为心脏疾病无创监测提供新的途径。

[0004] 早在1991年报道，Salerno等学者首次在临床中观察到心肌缺血患者的心脏振动谱异于正常人，并提出SCG(Seismocardiogram，SCG，由心脏运动对胸壁产生的加速度所绘制的图谱)可能对冠心病患者的左心室功能监测有帮助。科技人员进一步研究发现SCG能够估计出心脏的血流动力学参数，如射血前期时间、左室射血时间、射血分数等，进而评估心脏功能。

[0005] 大部分研究均局限于实验室环境下，2010年的MagIC-SCG是第一款可以在日常活动中连续采集心脏电机械信号的可穿戴设备。该系统包含两个ECG电极、一个压力传感器、一个三轴加速度传感器和一个数据储存及传输模块，所有模块被封装在一件特制的上衣内。数据通过蓝牙传输到计算机设备进行计算、分析和可视化。可以分析出的指标包括心率、呼吸次数和一些血流动力学参数。2017年中国台湾学者发明了一套基于多通道SCG和ECG联合分析的心脏疾病早期预警系统。其传感器包括三个ECG电极，4个加速度传感器，分布在人体四肢、胸壁等不同位置。传感器数据先传送至智能手机，再传输至云端服务器进行计算分析。通过对ECG和4通道SCG数据联合分析，最终达到88%的预警准确度。迄今为止，大部分学者是所采取的技术手段是将SCG和GCG(Gyrocardiography， GCG，由心脏运动对胸壁产生的旋转角速度所绘制的图谱)数据融合，取得了较好的效果。也有人直接采用智能手机内置的传感器，如Jafari Tadi等用智能手机内置的三轴加速度传感器和陀螺仪检测房颤，准确度也是很高的，但是数据计算和分析仍然需要离线进行。Ng Seng Hooi 等人2018年利

用加速度传感器对心脏瓣膜开合引起的振动进行监测分析，再一次验证了SCG对于心脏早期物理病变的预警价值，但整个实验停留在理论概念验证阶段，没有提出一套商业上可行的实施方案。

[0006] 综上所述，现有技术和产品存在着：其一数据分析处理和疾病诊断依赖于云端平台或离线计算机设备，实时性差，影响了即时响应，即时处置的实用性，数据可用性低。其二是配套的可穿戴设备结构复杂，成本高，使用不便。其三是软件算法模型简单，导致疾病诊断能力弱。其四未考虑数据安全性问题；其五没有考虑心脏预警，手术康复与居家养老等商业化服务模式。本发明人多年潜心研究心脏动态信号，尤其基于振动信号采集与分析，以及心脏疾病诊断方面的研究，让基于SCG+GCG的数据采集与分析技术的小型化与智能化，直接应用于远程心脏机能的动态预警，手术的康复、居家养老的心脏功能的实时跟踪服务的商业化网络系统研究与应用，为人类健康事业做一些实实在在的贡献。

发明内容

[0007] 本发明第一目的在于提供一种基于心脏功能动态监测与分析的数据加密-解密系统；另一目的在于提供基于心脏功能动态监测与分析的数据加密-解密方法。

[0008] 本发明第一目的是这样实现的，一种基于心脏功能动态监测与分析的数据加密-解密系统，所述数据加密-解密系统固化于心脏智能贴片中，具体包括，

所述特征ID装置，用于针对心脏智能贴片产生一个ID和256位的密钥对，标识一个心脏智能贴片，固化于心脏贴片中，作为其唯一身份识别密钥，存入数据库；

所述逻辑电路装置，用于对原始数据执行SHA(安全哈希算法)哈希算法，得到哈希值，附加在原始数据的末端形成明文，然后使用密钥对明文进行AES(高级加密算法)加密，得到密文，密文连同设备ID一起传输；

所述识别解密装置，用于接受密文和心脏智能贴片ID后，通过数据库查找出ID对应的密钥，进行解密。

[0009] 本发明另一目的是这样实现的，基于心脏功能动态监测与分析的数据加密-解密方法，具体包括下列步骤，

(1)通过所述特征ID装置标识生产一个ID和256位的密钥对，标识一个心脏智能贴片，固化于心脏贴片中，作为其唯一身份识别密钥，存入数据库；

(2)通过所述逻辑电路装置对原始数据执行SHA哈希算法，得到哈希值，附加在原始数据的末端形成明文，然后使用密钥对明文进行AES加密，得到密文，密文连同设备ID一起传输；

(3)通过所述识别解密装置，用于接受密文和心脏智能贴片ID后，通过数据库查找出ID对应的密钥，进行解密。从解密数据中分离出明文和哈希值，再次对明文进行同样的哈希算法，将计算得到哈希值与解密得到的哈希值进行对比，如果完全一致，则接受数据。

[0010] 本发明数据加密—解密技术应用于便携式心脏智能贴片系统，以可穿戴设备的形式佩戴于人体胸壁，对心脏机械振动进行体外监测，连续地、实时非侵入地获取心脏的振动信息，结合数字处理、机器学习和人工智能技术模式识别和智能诊断，早期发现心脏物理结构和搏动节律异常，如瓣膜病变、心脏壁的运动异常、心脏射血分数改变、心律失常等。结合预警报告系统，实现心脏疾病早预警与及时医护的目的。对严重心律失常(如房颤、室速、室

颤)、心绞痛、急性心肌梗死的早期预警监测,手术后康复监测,居家养老人群,体育运动人群的日常监护有着重大意义。

附图说明

[0011] 图1为本发明加密-解密系统架构关系框图;

图2为本发明之心脏智能贴片系统架构关系框图;

图3为本发明心脏智能贴片结构关系框图(方框内为智能芯片);

图4为本发明智能芯片的一种实现方式示意图。

具体实施方式

[0012] 下面将结合附图与实施例对本发明作进一步的说明,但不以任何方式对本发明加以限制,基于本发明的教导所作的任何变换或改变,均属于本发明保护的范围。

[0013] 如图1、2所示,本发明一种基于心脏功能动态监测与分析的数据加密-解密系统,所述数据加密-解密系统固化于心脏智能贴片中,具体包括,

所述特征ID装置,用于针对心脏智能贴片产生一个ID和256位的密钥对,标识一个心脏智能贴片,固化于心脏贴片中,作为其唯一身份识别密钥,存入数据库;

所述逻辑电路装置,用于对原始数据执行SHA-3哈希算法,得到哈希值,附加在原始数据的末端形成明文,然后使用密钥对明文进行AES加密,得到密文,密文连同设备ID一起传输;

所述识别解密装置,用于接受密文和心脏智能贴片ID后,通过数据库查找出ID对应的密钥,进行解密;

还包括所述识别接收装置,用于解密的数据再次哈希算法,校验哈希值,如果匹配,则接收数据;如果不匹配,说明数据可能被篡改,则拒绝接收,丢弃数据。

[0014] 还包括密文暂存装置,用于加密后的密文(即预警信息)的暂时存储,位于芯片存储器之闪存中。

[0015] 还包括预警启动装置,用于根据密文“携带预警事件信息”启动预警机制,并提示相应预警级别;同时移动智能终端的液晶显示屏显示文字和图标提示预警信息与级别。

[0016] 所述预警启动装置根据预警级别不同,显示预警状态:轻微预警时,黄灯闪烁;中等级别预警时,红灯闪烁;危急预警时,同时出现红灯闪烁和蜂鸣器响应。

[0017] 本发明基于心脏功能动态监测与分析的数据加密-解密方法,具体包括下列步骤,

(1)通过所述特征ID装置标识生产一个ID和256位的密钥对,标识一个心脏智能贴片,固化于心脏贴片中,作为其唯一身份识别密钥,存入数据库;

(2)通过所述逻辑电路装置对原始数据执行SHA-3哈希算法,得到哈希值,附加在原始数据的末端形成明文,然后使用密钥对明文进行AES加密,得到密文,密文连同设备ID一起传输;

(3)通过所述识别解密装置,用于接受密文和心脏智能贴片ID后,通过数据库查找出ID对应的密钥,进行解密;

还通过所述识别接收装置,将解密的数据再次执行哈希算法,校验哈希值,如果匹配,则接收数据;如果不匹配,说明数据可能被篡改,则拒绝接收,丢弃数据。

[0018] 还通过密文暂存装置将加密后的密文(即预警信息)暂时存储于芯片存储器之闪存中。

[0019] 还通过预警启动装置根据密文“携带预警事件信息”启动预警机制,并提示相应预警级别;并通过移动智能终端的液晶显示屏显示文字和图标提示预警信息与级别。

[0020] 通过所述预警启动装置启动预警机制,并根据预警级别不同作出不同的预警提示:轻微预警时,黄灯闪烁;中等级别预警时,红灯闪烁;危急预警时同时出现红灯闪烁并发出蜂鸣。

[0021] 下面通过实施例,说明本发明的工作原理与工作过程

本发明数据加密—解密技术应用于便携式心脏智能贴片系统,以可穿戴设备的形式佩戴于人体胸部正中位置,对心脏机械振动进行体外监测,连续地、实时非侵入地获取心脏的振动信息,结合数字处理、机器学习和人工智能技术模式识别和智能诊断,早期发现心脏物理结构和搏动节律异常,如瓣膜病变、心脏壁的运动异常、心脏射血分数改变、心律失常等。结合预警报告系统,实现心脏疾病早预警与及时医护的目的。

[0022] 图2、图3示出了应用本发明的心脏功能智能监测预警装置系统架构关系和装置结构关系。系统连续从振动传感器采集振波数据,实时进行数据压缩、数据预处理,嵌入式人工智能算法模块实时进行数据推断,给出诊心脏断结果。如果诊断结果存在异常(如发生心肌梗死、心律失常等),经过身份识别后,结果再经加密-解密系统进行加密后,暂存在内部的存储器内,并即时经数据通信模块将加密的诊断结果传输至智能终端或后台服务云平台等其他模块进行解密以及后续处理。这种数据传输方式称为基于“事件驱动”的数据传输,即只有在智能处理芯片逻辑电路检测到发生了心脏异常事件的情况下,才会开启数据传输,传输的数据包括诊断结论和事件发生时间前后一定时间段内的传感器原始数据,以便后续分析。

[0023] 所述微处理器采用片上系统SoC实现,SoC芯片中既包含处理器又包含存储器及外围电路,单个芯片就能实现数据的采集、转换、存储、处理和输入/输出等多种功能。

[0024] 所述微处理器为MCU(Microcontroller Unit)、专用集成芯片ASIC(Application Specific Integrated Circuit)或现场可编程门阵列FPGA;均可以实现本发明之目的。

所述电源管理装置包括纽扣型电池,并通过相关插口对系统供电;所述预警装置通过相关插口启动外置蜂鸣器、LED灯或液晶显示屏报警。

[0025] 所述无线数据通讯装置智采用无线方式进行数据传输,将发现的预警事件的相关信息经过256位AES加密后传送给蓝牙模块,或WiFi、4G、5G、NFC、NB-IoT模块,将无线信号通过隐形式天线发送。

[0026] 作为一种实施例,采用nRF52832蓝牙SoC芯片,该SoC芯片包含64MHZ的ARM Cortex-M4F CPU,512KB闪存,64KB RAM,低功耗蓝牙模块,2.4GHZ的无线发射模块,AHB/APB总线结构,以及相关的外围电路、接口和电源管理模块;所述智能贴片的传感器信息通过智能处理芯片的J7插口输入到16位200KSPS ADC端,A/D模块进行数模转换;智能处理芯片之微处理器模块对数据进行实时地预处理,然后进行实时数据计算推演,将推演结果存储、分发至相关子系统、平台或智能移动终端。所述智能处理芯片将预警结果经过256位AES加密后传送给蓝牙模块;蓝牙信号通过J9插口及隐形式天线发送。所述电源管理模块包括纽扣电池,容量不低于950mAh;通过SoC芯片J8插口对系统供电。

[0027] 心脏预警事件的编号会被加上时间标签以及当时所处地理位置坐标，进行哈希算法和AES加密处理，加密后的密文(即预警信息)会暂时存储在芯片上的闪存队列中，如果队列已满，则覆盖最旧的数据。然后立即启动芯片上的预警机制，根据预警级别不同，轻微预警时黄灯闪烁，中等级别预警时红灯闪烁，危急预警时同时出现红灯闪烁和发出蜂鸣。同时也可以加入液晶显示屏，通过文字和图标来显示预警信息。

[0028] 同时心脏智能贴片会尝试将预警数据通过无线网络传输至其他设备，如通过Wifi、NB-IoT、4G、5G等协议传输至云端后台服务器。如果在室内，还可以通过蓝牙、NFC等协议传输至智能手机或智能服务机器人。

[0029] 当云端服务器接受到预警信息后，首先会进行解密和存储，然后根据预警级别的不同，发出不同的预警信号：低度危险的可发送短信告知患者本人或监护人，高度危险的比如完全房室传导阻滞、心室颤动等会启动自动语音电话，通知监护人或医生。

[0030] 用户端手机APP在接受到预警信息后，会可视化展示当前的心脏诊断及建议，不同的预警级别会有不同的颜色显示，严重预警还会调用手机的振动器和扬声器。APP同时提供一键联系监护人和医生的按钮，可选择手机短信或电话方式，供用户在紧急情况下使用。APP还提供历史报告查看和添加、修改病情档案的功能。病情档案包括年龄、性别、身高、体重等个人基本信息，所患疾病信息，日常用药信息，以及医院检查、化验等资料。这些信息可以由用户授权远程共享给医生，以帮助医生更加准确的判断病情。此外，用户还可以在APP上添加或修改用于接受预警的监护人姓名、手机号码以及医生信息。手机APP和远端服务器之间会实时进行数据同步。

[0031] 医生端手机APP提供医生所管理用户列表，点击用户列表可查看用户的预警和档案等，还可选择以短信或电话的方式联系用户或其监护人，实现远程指导。

[0032] 对于某一些疾病，比如心房颤动，可能是长期或一段时间持续存在的，为了避免频繁预警造成打扰，系统可以设定不同的预警频率，比如1天最多1次等。对于急性心肌梗死等严重情况，预警频率不受限制。

[0033] 智能贴片在完成一次推断、数据加密及传输后，会循环工作，进入下一个运行周期。

[0034] 除了事件预警外，心脏智能贴片在工作期间，会定时(比如每小时)向后台服务器或手机APP发送加密消息，携带当时的工作状态和用户的心率信息。心率作为最基本的心脏参数，可以通过多种方式获取，如对心脏振动信号进行自相关分析、波峰查找算法等。

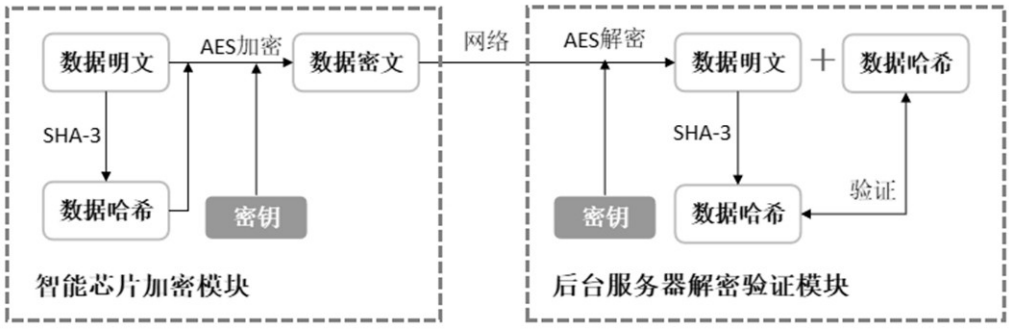

数据明文
AES加密
数据密文
网络
AES解密
数据明文
+
数据哈希
SHA-3
SHA-3
验证
数据哈希
密钥
密钥
数据哈希
智能芯片加密模块
后台服务器解密验证模块

图1

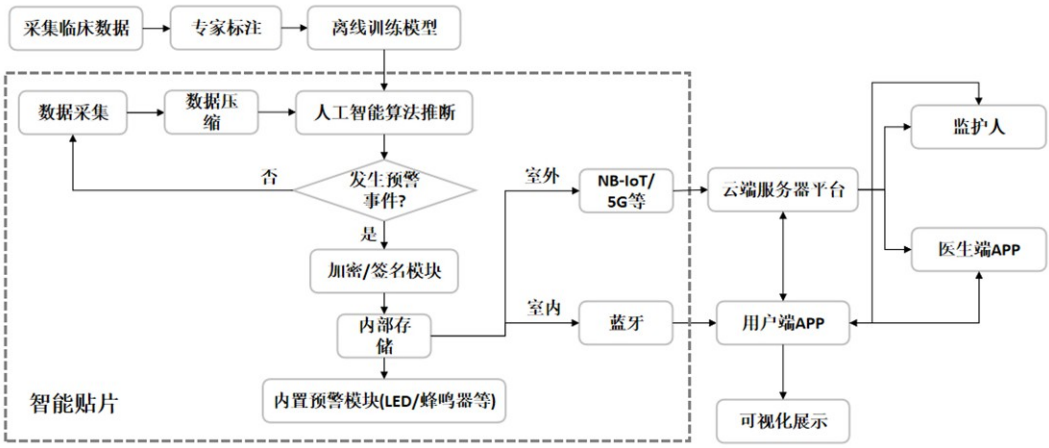

采集临床数据
专家标注
离线训练模型
数据采集
数据压缩
人工智能算法推断
否
发生预警事件?
是
室外
室内
NB-IoT/5G等
蓝牙
云端服务器平台
用户端APP
监护人
医生端APP
可视化展示
加密/签名模块
内部存储
内置预警模块(LED/蜂鸣器等)
智能贴片

图2

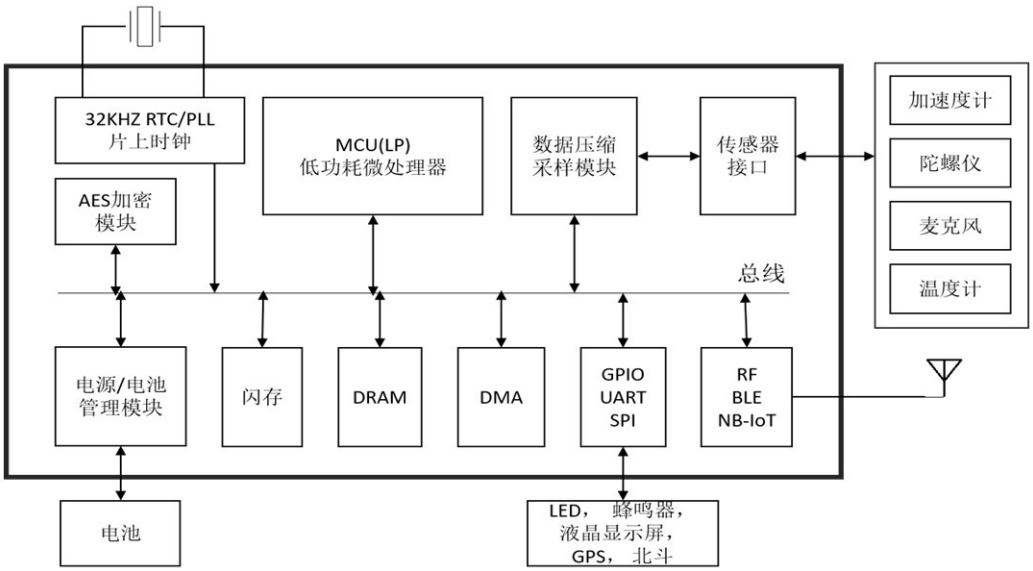

32KHZ RTC/PLL
片上时钟
MCU(LP)
低功耗微处理器
数据压缩
采样模块
传感器
接口
加速度计
陀螺仪
麦克风
温度计
AES加密
模块
总线
电源/电池
管理模块
闪存
DRAM
DMA
GPIO
UART
SPI
RF
BLE
NB-IoT
电池
LED， 蜂鸣器，
液晶显示屏，
GPS， 北斗

图3

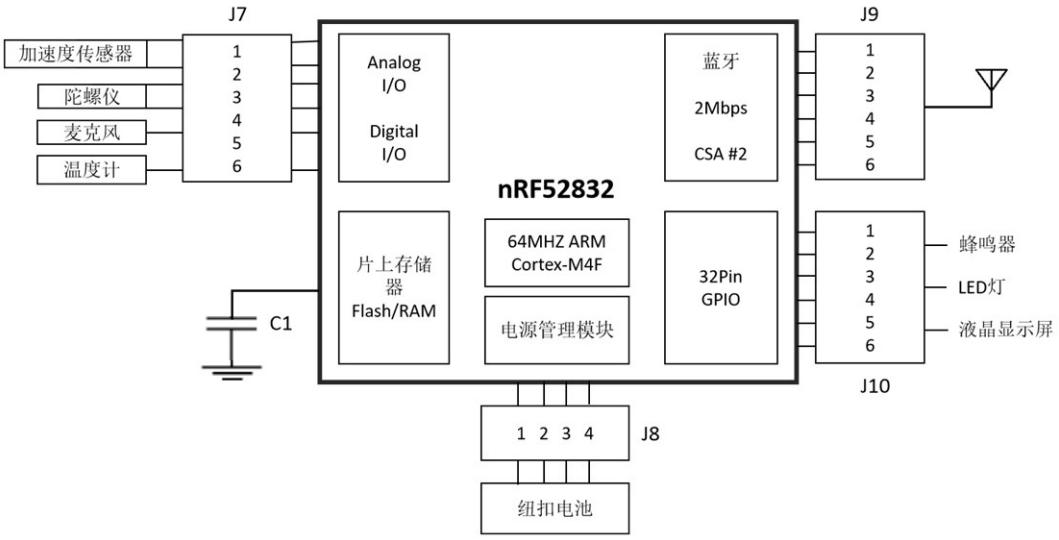

J7
加速度传感器
陀螺仪
麦克风
温度计
1
2
3
4
5
6
Analog
I/O
Digital
I/O
蓝牙
2Mbps
CSA #2
J9
nRF52832
片上存储
器
Flash/RAM
64MHZ ARM
Cortex-M4F
电源管理模块
32Pin
GPIO
蜂鸣器
LED灯
液晶显示屏
J10
C1
1 2 3 4
J8
纽扣电池

图4

专利名称(译)	一种基于心脏功能动态监测与分析的数据加密—解密系统及方法		
公开(公告)号	CN110598424A	公开(公告)日	2019-12-20
申请号	CN201910726569.9	申请日	2019-08-07
[标]申请(专利权)人(译)	王满 王江源		
申请(专利权)人(译)	王满 王江源		
当前申请(专利权)人(译)	王满 王江源		
[标]发明人	王江源 王满		
发明人	王江源 王满		
IPC分类号	G06F21/60 G06F21/62 A61B5/00 A61B5/024 A61B5/029 A61B5/11		
CPC分类号	A61B5/02405 A61B5/02438 A61B5/029 A61B5/1102 A61B5/6802 A61B5/7203 A61B5/725 A61B5/7264 A61B5/746 G06F21/602 G06F21/6245		
外部链接	Espacenet SIPO		

摘要(译)

本发明公开了一种基于心脏功能动态监测与分析的数据加密-解密系统及方法，包括特征ID装置、逻辑电路加密装置、识别解密装置，所述解密装置用于接受密文和心脏智能贴片ID后，通过数据库查找出ID对应的密钥，进行解密。本发明采用便携式智能可穿戴设备对心脏机械振动进行体外监测，实时非侵入地获取心脏的振动信息，结合数字处理、机器学习和人工智能技术模式识别和智能诊断，早期发现心脏物理结构和搏动节律异常，如瓣膜病变、心脏壁的运动异常、心脏射血分数改变、心律失常等。结合预警报告系统，实现心脏疾病早预警与及时医护的目的。对严重心律失常、心绞痛、急性心肌梗死的早期预警监测，对照手术后康复监测，居家养老人群，体育运动人群的日常监护意义重大。