



(12)发明专利

(10)授权公告号 CN 105975783 B

(45)授权公告日 2018.06.12

(21)申请号 201610313210.5

A61B 5/1172(2016.01)

(22)申请日 2016.05.12

A61B 5/00(2006.01)

(65)同一申请的已公布的文献号

A61B 5/145(2006.01)

申请公布号 CN 105975783 A

A61B 5/22(2006.01)

A61B 5/0476(2006.01)

(43)申请公布日 2016.09.28

(73)专利权人 宁波大学

地址 315211 浙江省宁波市江北区风华路
818号

(72)发明人 郑紫微 季克宇

(74)专利代理机构 宁波诚源专利事务所有限公
司 33102

代理人 刘凤钦

(51)Int.Cl.

G16H 40/67(2018.01)

G06Q 20/32(2012.01)

G06Q 20/38(2012.01)

G06Q 20/40(2012.01)

A61B 5/0205(2006.01)

(56)对比文件

CN 102906766 A,2013.01.30,

CN 102204306 A,2011.09.28,

CN 104113618 A,2014.10.22,

CN 103268422 A,2013.08.28,

CN 103279665 A,2013.09.04,

CN 1799493 A,2006.07.12,

CN 104173034 A,2014.12.03,

CN 104188641 A,2014.12.10,

US 2012239564 A1,2012.09.20,

US 9026462 B2,2015.05.05,

陈平顺 等.基于Android的NFC移动支付系
统设计与实现.《数据通信》.2015,

审查员 张红云

权利要求书5页 说明书14页 附图2页

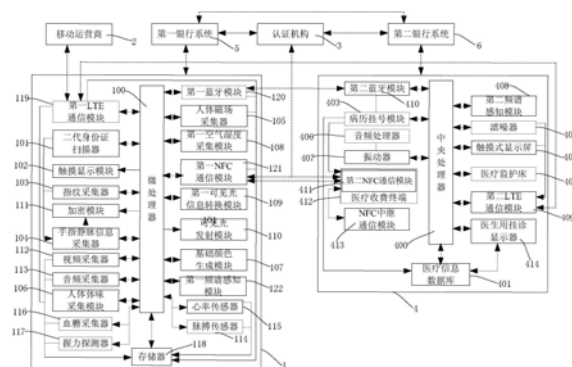
(54)发明名称

基于移动近场通信的医疗监护系统

(57)摘要

本发明涉及基于移动近场通信的医疗监护系统,其特征在于,包括移动智能终端、移动运营商、认证机构、医疗监护子系统、第一银行系统和第二银行系统;患者可利用移动智能终端与医生进行远程交互,还可将患者的心率、脉搏等信息一起发送给远端的医生,以供医生对病症做出准确诊断,移动智能终端与医疗收费终端在进行基于NFC的医疗费用支付时,移动智能终端以其构建的人体磁场数据库作为其合法拥有者操作该移动智能终端的身份识别信息,构建其合法拥有者体味数据库以及各手指所对应的静脉信息数据库,移动智能终端的合法拥有者以基础颜色为基础,设置其关于费用支付的二次确认支付密码,由此提高移动智能终端在医疗监护系统处支

付医疗费用的安全性能。



1. 基于移动近场通信的医疗监护系统,其特征在于,包括移动智能终端、移动运营商、认证机构、医疗监护子系统、第一银行系统和第二银行系统;其中:

所述移动智能终端包括微处理器及分别连接微处理器的二代身份证扫描器、触摸显示模块、指纹采集器、手指静脉信息采集器、人体磁场采集器、人体体味采集模块、基础颜色生成模块、第一空气湿度采集模块、第一可见光信息转换模块、可见光发射模块、加密模块、视频采集器、音频采集器、脉搏传感器、心率传感器、血糖采集器、握力探测器、存储器、第一LTE通信模块、第一蓝牙模块、第一NFC通信模块以及能够检测空闲频段的第一频谱感知模块,二代身份证扫描器、指纹采集器、手指静脉信息采集器分别连接加密模块,视频采集器、音频采集器、脉搏传感器、心率传感器、血糖采集器和握力探测器分别连接存储器;存储器分别连接第一LTE通信模块、第一蓝牙模块和第一NFC通信模块,视频采集器、音频采集器、脉搏传感器、心率传感器、血糖采集器和握力探测器分别连接第一LTE通信模块,第一LTE通信模块连接第一频谱感知模块;其中:

所述二代身份证扫描器,用以获取患者的身份证号码信息,并经加密模块加密后保存到存储器;所述指纹采集器,用以采集移动智能终端合法拥有者的指纹信息,以提前确认移动智能终端利用第一NFC通信模块完成支付交易的过程;所述视频采集器、音频采集器,用于分别对应获取患者的视频、音频信息,并在保存到存储器中的同时,利用第一LTE通信模块传送至医疗监护子系统;基础颜色生成模块,用于生成包括红色、橙色、黄色、绿色、青色、蓝色和紫色的七种基础颜色,并在触摸显示模块上进行显示,以供用户选择任意的颜色组合作为支付色;第一可见光信息转换模块,用以将数字信息转换为可见光后,以可见光形式发送出去;人体磁场采集器,用以检测人体磁场数据,并发送检测到的人体磁场数据给微处理器;人体体味采集模块,用以采集人体体味数据,并发送检测到的人体体味数据给微处理器;

所述医疗监护子系统包括中央处理器以及分别连接中央处理器的医疗信息数据库、医疗监护床、病历挂号模块、触摸式显示屏、滤噪器、音频处理器、振动器、第二频谱感知模块、第二LTE通信模块、第二蓝牙模块、具有第二NFC通信模块的医疗收费终端、M个NFC中继通信模块、医生用挂诊显示器,触摸式显示屏和滤噪器分别连接第二LTE通信模块,第二LTE通信模块连接第二频谱感知模块;第二蓝牙模块、第二NFC通信模块分别连接病历挂号模块,病历挂号模块连接医疗信息数据库,医疗信息数据库连接医生用挂诊显示器,音频处理器连接振动器,各NFC中继通信模块分别连接第二NFC通信模块,医疗监护床上设置有连接医疗信息数据库的监护控制器、脑电波采集装置、脑电波分析装置、脑电波控制装置、呼叫按钮、身体生理参数采集器、监护RFID标签、监护参数存储器、发光装置以及医疗监护床单,脑电波采集装置连接脑电波分析装置,医疗床单上设置有布料检测器和压力传感器阵列,身体生理参数采集器、监护RFID标签和压力传感器阵列均连接监护参数存储器,压力传感器阵列和布料检测器均连接监护控制器, $M \geq 2$;其中:

所述脑电波采集装置,用以采集瘫痪患者的脑电波信号,并发送给脑电波分析装置;脑电波分析装置,将接收的脑电波信号转换成预存的患者控制信号且发送给监护控制器,并由监护控制器控制医疗监护床上的其他部件;所述病历挂号模块,实现患者利用移动智能终端通过第一蓝牙模块、第二蓝牙模块配对通信后与其连接,并将挂号患者的身份证号码信息发送至医疗信息数据库存储;所述医疗信息数据库,用以根据挂号患者信息以及挂号

先后的顺序,按照挂号先后顺序发送患者信息给医生用挂诊显示器;所述医生用挂诊显示器,用以显示挂号患者信息,以供医生了解挂号患者信息;所述触摸式显示屏,用以显示所接收患者的远程视频,以供医生根据远程视频掌握患者基本病症情况;所述滤噪器,用以滤除所接收患者脉搏音频中的噪声,并将获取的纯净的脉搏音频发送给音频处理器处理;所述音频处理器,用以放大接收的纯净的脉搏音频,并提取放大后的脉搏音频的频率和振幅给中央处理器;所述第二频谱感知模块,用以检测医疗服务子系统周围处于空闲状态的通信频段,并发送给中央处理器;所述中央处理器,一方面在接收到音频处理器发送的脉搏音频振幅后,命令振动器按照一定频率和振幅做振动以重构患者脉搏,使医生在远端了解患者真实脉搏情况;一方面,根据接收的空闲通信频段值,命令第二LTE通信模块切换至空闲通信频段上传输;另一方面,获取具有最优中继性能的NFC中继通信模块作为最佳NFC中继通信模块;所述第二蓝牙模块,用以配对连接第一蓝牙模块,实现患者利用移动智能终端在蓝牙通信距离内即可及时完成挂号;所述医疗收费终端,用以通过最佳NFC中继通信模块以及第二NFC通信模块、第一NFC通信模块,完成移动智能终端与医疗收费终端的近场通信支付交易过程;其中,所述移动智能终端与医疗收费终端实现近场通信支付交易过程包括如下步骤:

步骤1,移动智能终端采集、存储其合法拥有者的身份证号码信息,并在预设的时间段内实时采集其合法拥有者的人体磁场数据,构建其合法拥有者在各预设时间段内的人体磁场数据库,并以构建的人体磁场数据库作为其合法拥有者的身份识别信息;其中,预设的时间段包括第一预设时间段和第二预设时间段,第一预设时间段为06:00至18:00;第二预设时间段为18:00至次日06:00;

步骤2,移动智能终端采集其合法拥有者的体味数据、接收其合法拥有者的各手指所对应的指纹信息和静脉信息,构建移动智能终端合法拥有者体味数据库以及各手指所对应的指纹信息数据库和静脉信息数据库;移动智能终端分别赋予其合法拥有者的人体磁场具有身份识别的第一优先级、体味数据具有身份识别的第二优先级;在识别操作者是否具有合法身份过程中,第一优先级具有比第二优先级更高的识别可信度;

步骤3,移动智能终端在其触摸显示屏上显示预设个数的支付密码输入框给其合法拥有者,各支付密码输入框均分别对应着七种供任意选择的基础颜色列表;其中,基础颜色列表中的七种基础颜色分别为红色、橙色、黄色、绿色、青色、蓝色和紫色,每个支付密码输入框对应着一组支付允许色;各组支付允许色为七种基础颜色的任意组合;

步骤4,根据触摸显示屏上各支付密码输入框对应的基础颜色列表,移动智能终端的合法拥有者依次选取自定义种类数的基础颜色组合分别作为各支付密码输入框的支付允许色,并由移动智能终端分别对应地存储各支付密码输入框所对应的支付允许色;移动智能终端的合法拥有者在每个支付密码输入框中对应输入的一组支付允许色的整体组合即形成该移动智能终端关于支付的二次确认支付密码;

步骤5,移动智能终端根据其合法拥有者的身份证号码信息以及关于支付的二次确认支付密码,生成表征移动智能终端合法拥有者对该移动智能终端合法拥有认证信息的身份认证密钥;其中,身份认证密钥标记为K,身份认证密钥K的获取过程包括步骤5-1至步骤5-5:

步骤5-1,移动智能终端提取其合法拥有者的身份证号码信息,并分别获取其身份证号

码信息中所有数字的身份证号码信息的累计和值、身份证号码信息的平均值以及身份证号码信息特征值;其中:

$$X = \sum_{i=1}^m x_i, \quad Y = \frac{1}{m} \sum_{i=1}^m x_i, \quad Z = \frac{X}{Y};$$

X为身份证号码信息的累计和值,Y为身份证号码信息的平均值,Z为身份证号码信息特征值; x_i 为身份证号码中的第i个数字,m为身份证号码信息中所有数字的个数;

步骤5-2,根据得到的身份证号码信息的累计和值、平均值以及身份证号码信息特征值,得到在预设时间段内有效的第一认证密钥值;第一认证密钥值标记为k,第一认证密钥值k由如下公式得到: $k^3 = Xt^2 + Yt + Z$; $t \in (T_1, T_2)$;

其中,t为移动智能终端的合法拥有者输入完毕二次确认支付密码的时刻, T_1 为身份认证密钥的预设时间段的起始时刻, T_2 为身份认证密钥的预设时间段的终止时刻;

步骤5-3,移动智能终端提取各支付密码输入框中对应的每组支付允许色,并计算得到各支付密码输入框中对应每组支付允许色的灰度平均值;其中,各支付密码输入框对应的一组支付允许色的灰度平均值I(n)由如下公式得到:

$$I(n) = \frac{1}{J_n} \sum_{j=1}^{J_n} I(n, j);$$

其中,I(n)为第n个支付密码输入框所对应组的支付允许色的灰度平均值, J_n 为第n个支付密码输入框中支付允许色所对应基础颜色的个数,I(n,j)为第n个支付密码输入框中第j个基础颜色的灰度值, $1 \leq j \leq J_n$;

步骤5-4,根据各支付密码输入框对应的一组支付允许色的灰度平均值,计算所有的支付密码输入框中支付允许色的灰度平均值I;其中:

$$I = \frac{1}{N} \sum_{n=1}^N I(n);$$

N为所有支付密码输入框的个数,I(n)为第n个支付密码输入框所对应的一组支付允许色的灰度平均值;

步骤5-5,根据得到的第一认证密钥值k以及支付允许色灰度平均值I,得到在预设时间段内有效的身份认证密钥,并将该身份认证密钥存储到移动智能终端中;身份认证密钥标记为K,身份认证密钥K由如下公式得到: $K^3 = Xt^2 + Yt + I$, $t \in [T_1, T_2]$;

t为移动智能终端的合法拥有者输入完毕二次确认支付密码的时刻, T_1 为身份认证密钥的预设时间段的起始时刻, T_2 为身份认证密钥的预设时间段的终止时刻;

步骤6,移动智能终端发送其第一NFC通信模块的真实身份标识号给认证机构,由认证机构生成移动智能终端交易用的匿名身份标识号;医疗收费终端发送其第二NFC通信模块的真实身份标识号给认证机构,由认证机构生成医疗收费终端交易用的匿名身份标识号;其中,移动智能终端的真实身份标识号记为Mobile_{id},认证机构标记为TSM,移动智能终端的匿名身份标识号记为Mobile_{aid},医疗收费终端的真实身份标识号记为Medical_{id},医疗收费终端的匿名身份标识号记为Medical_{aid};

Mobile_{aid} = sH(Mobile_{id}), Medical_{aid} = sH(Medical_{id}); sH(•)为哈希匿名函数;

步骤7,移动智能终端在第一银行系统注册其付款账户,医疗监护子系统在第二银行系统注册其收款账户,并作为医疗收费终端的收款账户;其中,移动智能终端的付款账户记为

Mobile_{acct}, 医疗监护子系统的收款账户记为Medical_{acct};

步骤8, 移动智能终端靠近医疗收费终端至近场通信距离以内时, 医疗收费终端首先开启近场通信请求, 并发送包括可选支付费用清单的支付交易初步认证信息给移动智能终端, 用户通过移动智能终端选择所需支付费用名称, 然后反馈所需支付费用名称给医疗收费终端, 从而开启移动智能终端与医疗收费终端的正式支付交易;

步骤9, 医疗收费终端根据移动智能终端所需支付费用名称, 发送包括对应该费用名称的支付金额、收据单号、医疗收费终端的匿名身份标识号、当前位置空气湿度、收据单号生成时间以及其与认证机构共享密钥的交易信息给移动智能终端; 其中, 该交易信息标记为E_{Medical}, $E_{\text{Medical}} = E(\text{ReceiptNum}, \text{Price}, \text{Medicalaid}, \text{RH}_{\text{Medical}}, T, K_{\text{Medical-TSM}})$;

ReceiptNum为医疗收费终端生成的收据单号; Price为移动智能终端需要支付的金额, Medicalaid为医疗收费终端的匿名身份标识号, RH_{Medical}为医疗收费终端当前位置空气湿度, T为收据单号生成时间; K_{Medical-TSM}为医疗收费终端与认证机构的共享密钥;

步骤10, 医疗收费终端发送包括步骤9中交易信息、医疗监护子系统收款账户以及其与认证机构间的共享密钥的认证信息给认证结构, 移动智能终端发送支付认证信息给认证结构; 其中, 移动智能终端发送的支付认证信息包括其临时识别码TMSI、其与认证机构间的共享密钥K_{Mobile-TSM}、其位置区识别码LAI、其当前位置空气湿度RH_{Mobile}、移动智能终端付款账户Mobile_{acct}及医疗收费终端发送的交易信息; 移动智能终端发送的支付认证信息记为E_{Mobile}; 其中:

$$E_{\text{Mobile}} = E(\text{ReceiptNum}, \text{Price}, \text{Medicalaid}, \text{Mobileaid}, \text{RH}_{\text{Medical}}, \text{RH}_{\text{Mobile}}, T, \text{TMSI}, \text{LAI}, K_{\text{Mobile-TSM}});$$

步骤11, 认证机构提取医疗收费终端所发送信息中的医疗收费终端匿名身份标识号, 并基于认证结构中已存储的医疗收费终端真实身份标识号进行匹配判断;

当认证机构利用医疗收费终端真实身份标识号以及哈希匿名函数所生成的医疗收费终端匿名身份标识号与提取的医疗收费终端匿名身份标识号匹配一致时, 表明发送该认证信息的医疗收费终端可信, 则认证机构执行步骤12; 否则, 认证机构切断与该认证信息所对应医疗收费终端之间的通信, 并发送包含此医疗收费终端匿名身份标识号的警告信息给移动智能终端;

步骤12, 认证机构提取移动智能终端支付认证信息中的临时识别码和位置区识别码, 并发送包括移动智能终端临时识别码、位置区识别码以及其与移动运营商间的共享密钥的反馈认证信息给移动运营商; 其中, 反馈认证信息记为E_{MNO}, $E_{\text{MNO}} = E(\text{TMSI}, \text{LAI}, K_{\text{TSM-MNO}})$; K_{TSM-MNO}表示认证机构与移动运营商之间的共享密钥;

步骤13, 移动运营商利用其与认证机构间的共享密钥提取反馈认证信息中的移动智能终端临时识别码和位置区识别码, 并根据移动智能终端临时识别码检索得到对应该临时识别码的移动用户识别码后, 发送包括移动智能终端临时识别码、位置区识别码以及移动用户识别码的已认证信息给认证机构;

步骤14, 认证机构提取认证信息中所含有的医疗收费终端当前位置空气湿度以及支付认证信息中所含有的移动智能终端当前位置空气湿度, 并判断医疗收费终端当前位置空气湿度与移动智能终端当前位置空气湿度之差低于预设的空气湿度差阈值时, 则认证机构发送确认支付命令信息给第一银行系统; 其中:

所述确认支付命令信息包括需扣除金额、收据单号、收据单号生成时间、移动智能终端支付账户、医疗监护子系统收款账户以及认证机构与第一银行系统间的共享秘钥；确认支付命令信息记为 E_{Confirm} ，其中：

$$E_{\text{Confirm}} = (\text{Amt}_{\text{dedt}}, \text{ReceiptNum}, T, \text{Mobile}_{\text{acct}}, \text{Medical}_{\text{acct}}, K_{\text{TSM-BANK1}});$$

其中， Amt_{dedt} 为移动智能终端支付账户应扣除的金额， $K_{\text{TSM-BANK1}}$ 为认证机构与第一银行系统间的共享秘钥，第一银行系统标记为 BANK_1 ；

步骤15，第一银行系统根据认证机构所发送的确认支付命令信息以及对应的应扣除金额，在移动智能终端的支付账户中，预扣除对应的金额，并将移动智能终端支付账户中扣除的金额预转移至医疗监护子系统在第二银行系统的收款账户中，并在完成操作后，第一银行系统发送包括扣款金额、扣款时间、银行授权扣款单号、扣款账户、收款账户以及共享秘钥的预扣款回执信息给移动智能终端进行存储，并转至步骤14进行二次支付确认操作；

步骤16，移动智能终端采集握持该移动智能终端人员的人体磁场强度、体味数据、指纹信息以及此时的时间值，并对该握持人员的身份进行鉴定判别：

当移动智能终端判断此时采集的人体磁场强度存在于移动智能终端已存储的该时间所对应预设时间段内的人体磁场强度数据库，且此时采集的体味数据同样存储于移动智能终端已存储的体味数据库中时，表明该握持人员为移动智能终端的合法拥有者，则移动智能终端执行步骤17；否则，移动智能终端在预设时间段内拒绝该握持人员对移动智能终端的任何操作；

步骤17，移动智能终端在其触摸显示屏显示各支付密码输入框以及对应各支付密码框的基础颜色列表，并在握持人员依次输入各组支付允许后，移动智能终端根据该握持人员输入的各支付密码输入框中的支付允许色进行判断：

当各支付密码输入框中的支付允许色与移动智能终端在步骤4中已对应存储的支付允许色完全一致时，表明输入了正确的二次确认支付密码，则移动智能终端执行步骤17；否则，表明输入了错误的二次确认支付密码，则移动智能终端在预设时间段内拒绝该握持人员对移动智能终端的任何操作；

步骤18，移动智能终端要求该握持人员输入其身份证号码信息，并基于该握持人员的身份证号码信息生成对应的身份认证秘钥 K' ，移动智能终端判断此时生成的身份认证秘钥 K' 与其已存储的身份认证秘钥 K 一致时，则移动智能终端发送确认转账命令给第一银行系统；否则，移动智能终端在预设时间段内拒绝该握持人员对该移动智能终端的任何关于支付的操作；

步骤19，第一银行系统在接收到移动智能终端所发送的支付命令后，第一银行系统转移步骤15中对应的款项给医疗监护子系统的收款账户，并在第二银行系统收到第一银行系统所转移的款项后，发送包括收款金额 Amt_{dedt} 、银行授权收款单号 $\text{BANK}_{\text{Trans}}$ 、收款账户 $\text{Medical}_{\text{acct}}$ 和收款时间 T_3 的收款回执信息给医疗监护子系统；收款回执信息标记为 E_{Receipt} ，其中， $E_{\text{Receipt}} = E(\text{Amt}_{\text{dedt}}, \text{BANK}_{\text{Trans}}, \text{Medical}_{\text{acct}}, T_3)$ 。

基于移动近场通信的医疗监护系统

技术领域

[0001] 本发明涉及医疗监护领域,尤其涉及一种基于移动近场通信的医疗监护系统。

背景技术

[0002] 在日常生活中,患者需要去医疗机构看病时,通常需要耗费较多时间排队挂号,然后排队等候医生的诊断,另外也需要耗费时间排队支付医疗费用。患者在医疗机构看病过程中,更多的时间耽误在排队上,这对轻微的患者虽然没有严重影响,但是对于一些病情较急或较重者,无疑是严重地影响了诊断和治疗效果。虽然,医疗机构有急诊科室,可以为少数急诊患者提供治疗。但是,由于医疗机构看病患者较多,如何缩短患者排队挂号时间以及费用支付时间,提高整个医疗机构的医疗监护效率,成为当前传统医疗需要必须面对的课题。

[0003] 随着近场通信(Near Field Communication,简称NFC)技术的不断兴起与日益成熟,将NFC技术应用到医疗监护系统中,从而既能方便患者及时挂号并得到医疗监护,医生及时掌握患者基本病症信息,又可以实现患者在医疗一端安全、及时完成费用支付成为现代医疗监护系统的新趋势。

发明内容

[0004] 本发明所要解决的技术问题是针对上述现有技术提供一种既可以方便患者及时挂号并得到医疗监护,医生及时掌握患者基本病症信息,又可以实现患者在医疗一端安全、及时完成费用支付的基于移动近场通信的医疗监护系统。

[0005] 本发明解决上述技术问题所采用的技术方案为:基于移动近场通信的医疗监护系统,其特征在于,包括移动智能终端、移动运营商、认证机构、医疗监护子系统、第一银行系统和第二银行系统;其中:

[0006] 所述移动智能终端包括微处理器及分别连接微处理器的二代身份证扫描器、触摸显示模块、指纹采集器、手指静脉信息采集器、人体磁场采集器、人体体味采集模块、基础颜色生成模块、第一空气湿度采集模块、第一可见光信息转换模块、可见光发射模块、加密模块、视频采集器、音频采集器、脉搏传感器、心率传感器、血糖采集器、握力探测器、存储器、第一LTE通信模块、第一蓝牙模块、第一NFC通信模块以及能够检测空闲频段的第一频谱感知模块,二代身份证扫描器、指纹采集器、手指静脉信息采集器分别连接加密模块,视频采集器、音频采集器、脉搏传感器、心率传感器、血糖采集器和握力探测器分别连接存储器;存储器分别连接第一LTE通信模块、第一蓝牙模块和第一NFC通信模块,视频采集器、音频采集器、脉搏传感器、心率传感器、血糖采集器和握力探测器分别连接第一LTE通信模块,第一LTE通信模块连接第一频谱感知模块;其中:

[0007] 所述二代身份证扫描器,用以获取患者的身份证号码信息,并经加密模块加密后保存到存储器;所述指纹采集器,用以采集移动智能终端合法拥有者的指纹信息,以提前确认移动智能终端利用第一NFC通信模块完成支付交易的过程;所述视频采集器、音频采集

器,用于分别对应获取患者的视频、音频信息,并在保存到存储器中的同时,利用第一LTE通信模块传送至医疗监护子系统;基础颜色生成模块,用于生成包括红色、橙色、黄色、绿色、青色、蓝色和紫色的七种基础颜色,并在触摸显示模块上进行显示,以供用户选择任意的颜色组合作为支付色;第一可见光信息转换模块,用以将数字信息转换为可见光后,以可见光形式发送出去;人体磁场采集器,用以检测人体磁场数据,并发送检测到的人体磁场数据给微处理器;人体体味采集模块,用以采集人体体味数据,并发送检测到的人体体味数据给微处理器;

[0008] 所述医疗监护子系统包括中央处理器以及分别连接中央处理器的医疗信息数据库、医疗监护床、病历挂号模块、触摸式显示屏、滤噪器、音频处理器、振动器、第二频谱感知模块、第二LTE通信模块、第二蓝牙模块、具有第二NFC通信模块的医疗收费终端、M个NFC中继通信模块、医生用挂诊显示器,触摸式显示屏和滤噪器分别连接第二LTE通信模块,第二LTE通信模块连接第二频谱感知模块;第二蓝牙模块、第二NFC通信模块分别连接病历挂号模块,病历挂号模块连接医疗信息数据库,医疗信息数据库连接医生用挂诊显示器,音频处理器连接振动器,各NFC中继通信模块分别连接第二NFC通信模块,医疗监护床上设置有连接医疗信息数据库的监护控制器、脑电波采集装置、脑电波分析装置、脑电波控制装置、呼叫按钮、身体生理参数采集器、监护RFID标签、监护参数存储器、发光装置以及医疗监护床单,脑电波采集装置连接脑电波分析装置,医疗床单上设置有布料检测器和压力传感器阵列,身体生理参数采集器、监护RFID标签和压力传感器阵列均连接监护参数存储器,压力传感器阵列和布料检测器均连接监护控制器, $M \geq 2$,其中:

[0009] 所述脑电波采集装置,用以采集瘫痪患者的脑电波信号,并发送给脑电波分析装置;脑电波分析装置,将接收的脑电波信号转换成预存的患者控制信号且发送给监护控制器,并由监护控制器控制医疗监护床上的其他部件;所述病历挂号模块,实现患者利用移动智能终端通过第一蓝牙模块、第二蓝牙模块配对通信后与其连接,并将挂号患者的身份证号码信息发送至医疗信息数据库存储;所述医疗信息数据库,用以根据挂号患者信息以及挂号先后的顺序,按照挂号先后顺序发送患者信息给医生用挂诊显示器;所述医生用挂诊显示器,用以显示挂号患者信息,以供医生了解挂号患者信息;所述触摸式显示屏,用以显示所接收患者的远程视频,以供医生根据远程视频掌握患者基本病症情况;所述滤噪器,用以滤除所接收患者脉搏音频中的噪声,并将获取的纯净的脉搏音频发送给音频处理器处理;所述音频处理器,用以放大接收的纯净的脉搏音频,并提取放大后的脉搏音频的频率和振幅给中央处理器;所述第二频谱感知模块,用以检测医疗服务子系统周围处于空闲状态的通信频段,并发送给中央处理器;所述中央处理器,一方面在接收到音频处理器发送的脉搏音频振幅后,命令振动器按照一定频率和振幅做振动以重构患者脉搏,使医生在远端了解患者真实脉搏情况;一方面,根据接收的空闲通信频段值,命令第二LTE通信模块切换至空闲通信频段上传输;另一方面,获取具有最优中继性能的NFC中继通信模块作为最佳NFC中继通信模块;所述第二蓝牙模块,用以配对连接第一蓝牙模块,实现患者利用移动智能终端在蓝牙通信距离内即可及时完成挂号;所述医疗收费终端,用以通过最佳NFC中继通信模块以及第二NFC通信模块、第一NFC通信模块,完成移动智能终端与医疗收费终端的近场通信支付交易过程;其中,所述移动智能终端与医疗收费终端实现近场通信支付交易过程包括如下步骤:

[0010] 步骤1,移动智能终端采集、存储其合法拥有者的身份证号码信息,并在预设的时间段内实时采集其合法拥有者的人体磁场数据,构建其合法拥有者在各预设时间段内的人体磁场数据库,并以构建的人体磁场数据库作为其合法拥有者的身份识别信息;其中,预设的时间段包括第一预设时间段和第二预设时间段,第一预设时间段为06:00至18:00;第二预设时间段为18:00至次日06:00;

[0011] 步骤2,移动智能终端采集其合法拥有者的体味数据、接收其合法拥有者的各手指所对应的指纹信息和静脉信息,构建移动智能终端合法拥有者体味数据库以及各手指所对应的指纹信息数据库和静脉信息数据库;移动智能终端分别赋予其合法拥有者的人体磁场具有身份识别的第一优先级、体味数据具有身份识别的第二优先级;在识别操作者是否具有合法身份过程中,第一优先级具有比第二优先级更高的识别可信度;

[0012] 步骤3,移动智能终端在其触摸显示屏上显示预设个数的支付密码输入框给其合法拥有者,各支付密码输入框均分别对应着七种供任意选择的基础颜色列表;其中,基础颜色列表中的七种基础颜色分别为红色、橙色、黄色、绿色、青色、蓝色和紫色,每个支付密码输入框对应着一组支付允许色;各组支付允许色为七种基础颜色的任意组合;

[0013] 步骤4,根据触摸显示屏上各支付密码输入框对应的基础颜色列表,移动智能终端的合法拥有者依次选取自定义种类数的基础颜色组合分别作为各支付密码输入框的支付允许色,并由移动智能终端分别对应地存储各支付密码输入框所对应的支付允许色;移动智能终端的合法拥有者在每个支付密码输入框中对应输入的各组支付允许色的整体组合即形成该移动智能终端关于支付的二次确认支付密码;

[0014] 步骤5,移动智能终端根据其合法拥有者的身份证号码信息以及关于支付的二次确认支付密码,生成表征移动智能终端合法拥有者对该移动智能终端合法拥有认证信息的身份认证密钥;其中,身份认证密钥标记为K,身份认证密钥K的获取过程包括步骤5-1至步骤5-5:

[0015] 步骤5-1,移动智能终端提取其合法拥有者的身份证号码信息,并分别获取其身份证号码信息中所有数字的身份证号码信息的累计和值、身份证号码信息的平均值以及身份证号码信息特征值;其中:

$$[0016] \quad X = \sum_{i=1}^m x_i, \quad Y = \frac{1}{m} \sum_{i=1}^m x_i, \quad Z = \frac{X}{Y};$$

[0017] X为身份证号码信息的累计和值,Y为身份证号码信息的平均值,Z为身份证号码信息特征值; x_i 为身份证号码中的第i个数字,m为身份证号码信息中所有数字的个数;

[0018] 步骤5-2,根据得到的身份证号码信息的累计和值、平均值以及身份证号码信息特征值,得到在预设时间段内有效的第一认证密钥值;第一认证密钥值标记为k,第一认证密钥值k由如下公式得到: $k^3 = Xt^2 + Yt + Z$; $t \in (T_1, T_2)$;其中,t为移动智能终端的合法拥有者输入完毕二次确认支付密码的时刻, T_1 为身份认证密钥的预设时间段的起始时刻, T_2 为身份认证密钥的预设时间段的终止时刻;

[0019] 步骤5-3,移动智能终端提取各支付密码输入框中对应的每组支付允许色,并计算得到各支付密码输入框中对应每组支付允许色的灰度平均值;其中,各支付密码输入框对应的一组支付允许色的灰度平均值I(n)由如下公式得到:

$$[0020] \quad I(n) = \frac{1}{J_n} \sum_{j=1}^{J_n} I(n, j);$$

[0021] 其中, $I(n)$ 为第 n 个支付密码输入框所对应组的支付允许色的灰度平均值, J_n 为第 n 个支付密码输入框中支付允许色所对应基础颜色的个数, $I(n, j)$ 为第 n 个支付密码输入框中第 j 个基础颜色的灰度值, $1 \leq j \leq J_n$;

[0022] 步骤5-4, 根据各支付密码输入框对应的一组支付允许色的灰度平均值, 计算所有的支付密码输入框中支付允许色的灰度平均值 I ; 其中:

$$[0023] \quad I = \frac{1}{N} \sum_{n=1}^N I(n);$$

[0024] N 为所有支付密码输入框的个数, $I(n)$ 为第 n 个支付密码输入框所对应的一组支付允许色的灰度平均值;

[0025] 步骤5-5, 根据得到的第一认证秘钥值 k 以及支付允许色灰度平均值 I , 得到在预设时间段内有效的身份认证秘钥, 并将该身份认证秘钥存储到移动智能终端中; 身份认证秘钥标记为 K , 身份认证秘钥 K 由如下公式得到: $K^3 = Xt^2 + Yt + I$, $t \in [T_1, T_2]$; t 为移动智能终端的合法拥有者输入完毕二次确认支付密码的时刻, T_1 为身份认证秘钥的预设时间段的起始时刻, T_2 为身份认证秘钥的预设时间段的终止时刻;

[0026] 步骤6, 移动智能终端发送其第一NFC通信模块的真实身份标识号给认证机构, 由认证机构生成移动智能终端交易用的匿名身份标识号; 医疗收费终端发送其第二NFC通信模块的真实身份标识号给认证机构, 由认证机构生成医疗收费终端交易用的匿名身份标识号; 其中, 移动智能终端的真实身份标识号记为 $Mobile_{id}$, 认证机构标记为 TSM , 移动智能终端的匿名身份标识号记为 $Mobile_{aid}$, 医疗收费终端的真实身份标识号记为 $Medical_{id}$, 医疗收费终端的匿名身份标识号记为 $Medical_{aid}$;

[0027] $Mobile_{aid} = sH(Mobile_{id})$, $Medical_{aid} = sH(Medical_{id})$; $sH(\cdot)$ 为哈希匿名函数;

[0028] 步骤7, 移动智能终端在第一银行系统注册其付款账户, 医疗监护子系统在第二银行系统注册其收款账户, 并作为医疗收费终端的收款账户; 其中, 移动智能终端的付款账户记为 $Mobile_{acct}$, 医疗监护子系统的收款账户记为 $Medical_{acct}$;

[0029] 步骤8, 移动智能终端靠近医疗收费终端至近场通信距离以内时, 医疗收费终端首先开启近场通信请求, 并发送包括可选支付费用清单的支付交易初步认证信息给移动智能终端, 用户通过移动智能终端选择所需支付费用名称, 然后反馈所需支付费用名称给医疗收费终端, 从而开启移动智能终端与医疗收费终端的正式支付交易;

[0030] 步骤9, 医疗收费终端根据移动智能终端所需支付费用名称, 发送包括对应该费用名称的支付金额、收据单号、医疗收费终端的匿名身份标识号、当前位置空气湿度、收据单号生成时间以及其与认证机构共享秘钥的交易信息给移动智能终端; 其中, 该交易信息标记为 $E_{Medical}$, $E_{Medical} = E(ReceiptNum, Price, Medical_{aid}, RH_{Medical}, T, K_{Medical-TSM})$;

[0031] $ReceiptNum$ 为医疗收费终端生成的收据单号; $Price$ 为移动智能终端需要支付的金额, $Medical_{aid}$ 为医疗收费终端的匿名身份标识号, $RH_{Medical}$ 为医疗收费终端当前位置空气湿度, T 为收据单号生成时间; $K_{Medical-TSM}$ 为医疗收费终端与认证机构的共享秘钥;

[0032] 步骤10, 医疗收费终端发送包括步骤9中交易信息、医疗监护子系统收款账户以及其与认证机构间的共享秘钥的认证信息给认证结构, 移动智能终端发送支付认证信息给认

证结构;其中,移动智能终端发送的支付认证信息包括其临时识别码TMSI、其与认证机构间的共享密钥 $K_{\text{Mobile-TSM}}$ 、其位置区识别码LAI、其当前位置空气湿度 RH_{Mobile} 、移动智能终端付款账户 $\text{Mobile}_{\text{acct}}$ 及医疗收费终端发送的交易信息;移动智能终端发送的支付认证信息记为 E_{Mobile} ;其中:

$$[0033] \quad E_{\text{Mobile}} = E(\text{ReceiptNum}, \text{Price}, \text{Medical}_{\text{aid}}, \text{Mobile}_{\text{aid}}, \text{RH}_{\text{Medical}}, \text{RH}_{\text{Mobile}}, T, \text{TMSI}, \text{LAI}, K_{\text{Mobile-TSM}});$$

[0034] 步骤11,认证机构提取医疗收费终端所发送信息中的医疗收费终端匿名身份标识号,并基于认证结构中已存储的医疗收费终端真实身份标识号进行匹配判断:

[0035] 当认证机构利用医疗收费终端真实身份标识号以及哈希匿名函数所生成的医疗收费终端匿名身份标识号与提取的医疗收费终端匿名身份标识号匹配一致时,表明发送该认证信息的医疗收费终端可信,则认证机构执行步骤12;否则,认证机构切断与该认证信息所对应医疗收费终端之间的通信,并发送包含此医疗收费终端匿名身份标识号的警告信息给移动智能终端;

[0036] 步骤12,认证机构提取移动智能终端支付认证信息中的临时识别码和位置区识别码,并发送包括移动智能终端临时识别码、位置区识别码以及其与移动运营商间的共享密钥的反馈认证信息给移动运营商;其中,反馈认证信息记为 E_{MNO} , $E_{\text{MNO}} = E(\text{TMSI}, \text{LAI}, K_{\text{TSM-MNO}})$; $K_{\text{TSM-MNO}}$ 表示认证机构与移动运营商之间的共享密钥;

[0037] 步骤13,移动运营商利用其与认证机构间的共享密钥提取反馈认证信息中的移动智能终端临时识别码和位置区识别码,并根据移动智能终端临时识别码检索得到对应该临时识别码的移动用户识别码后,发送包括移动智能终端临时识别码、位置区识别码以及移动用户识别码的已认证信息给认证机构;

[0038] 步骤14,认证机构提取认证信息中所含有的医疗收费终端当前位置空气湿度以及支付认证信息中所含有的移动智能终端当前位置空气湿度,并判断医疗收费终端当前位置空气湿度与移动智能终端当前位置空气湿度之差低于预设的空气湿度差阈值时,则认证机构发送确认支付命令信息给第一银行系统;其中,所述确认支付命令信息包括需扣除金额、收据单号、收据单号生成时间、移动智能终端支付账户、医疗监护子系统收款账户以及认证机构与第一银行系统间的共享密钥;确认支付命令信息记为 E_{Confirm} ,其中:

$$[0039] \quad E_{\text{Confirm}} = (\text{Amt}_{\text{dedt}}, \text{ReceiptNum}, T, \text{Mobile}_{\text{acct}}, \text{Medical}_{\text{acct}}, K_{\text{TSM-BANK}_1});$$

[0040] 其中, Amt_{dedt} 为移动智能终端支付账户应扣除的金额, $K_{\text{TSM-BANK}_1}$ 为认证机构与第一银行系统间的共享密钥,第一银行系统标记为 BANK_1 ;

[0041] 步骤15,第一银行系统根据认证机构所发送的确认支付命令信息以及对应的应扣除金额,在移动智能终端的支付账户中,预扣除对应的金额,并将移动智能终端支付账户中扣除的金额预转移至医疗监护子系统在第二银行系统的收款账户中,并在完成操作后,第一银行系统发送包括扣款金额、扣款时间、银行授权扣款单号、扣款账户、收款账户以及共享密钥的预扣款回执信息给移动智能终端进行存储,并转至步骤14进行二次支付确认操作;

[0042] 步骤16,移动智能终端采集握持该移动智能终端人员的人体磁场强度、体味数据、指纹信息以及此时的时间值,并对该握持人员的身份进行鉴定判别:

[0043] 当移动智能终端判断此时采集的人体磁场强度存在于移动智能终端已存储的该

时间所对应预设时间段内的人体磁场强度数据库,且此时采集的体味数据同样存储于移动智能终端已存储的体味数据库中时,表明该握持人员为移动智能终端的合法拥有者,则移动智能终端执行步骤17;否则,移动智能终端在预设时间段内拒绝该握持人员对移动智能终端的任何操作;

[0044] 步骤17,移动智能终端在其触摸显示屏显示各支付密码输入框以及对应各支付密码框的基础颜色列表,并在握持人员依次输入各组支付允许后,移动智能终端根据该握持人员输入的各支付密码输入框中的支付允许色进行判断:

[0045] 当各支付密码输入框中的支付允许色与移动智能终端在步骤4中已对应存储的支付允许色完全一致时,表明输入了正确的二次确认支付密码,则移动智能终端执行步骤17;否则,表明输入了错误的二次确认支付密码,则移动智能终端在预设时间段内拒绝该握持人员对移动智能终端的任何操作;

[0046] 步骤18,移动智能终端要求该握持人员输入其身份证号码信息,并基于该握持人员的身份证号码信息生成对应的身份认证密钥 K' ,移动智能终端判断此时生成的身份认证密钥 K' 与其已存储的身份认证密钥 K 一致时,则移动智能终端发送确认转账命令给第一银行系统;否则,移动智能终端在预设时间段内拒绝该握持人员对该移动智能终端的任何关于支付的操作;

[0047] 步骤19,第一银行系统在接收到移动智能终端所发送的支付命令后,第一银行系统转移步骤15中对应的款项给医疗监护子系统的收款账户,并在第二银行系统收到第一银行系统所转移的款项后,发送包括收款金额 Amt_{dedt} 、银行授权收款单号 $BANK_{Trans}$ 、收款账户 $Medical_{acct}$ 和收款时间 T_3 的收款回执信息给医疗监护子系统;收款回执信息标记为 $E_{Receipt}$,其中, $E_{Receipt} = E(Amt_{dedt}, BANK_{Trans}, Medical_{acct}, T_3)$ 。

[0048] 与现有技术相比,本发明的优点在于:

[0049] 首先,该医疗监护系统通过引入近场通信技术,使患者或者患者家属利用移动智能终端提前完成挂号以及费用支付;

[0050] 其次,在远程诊断过程中,患者可利用移动智能终端与医生进行远程交互,移动智能终端还可将患者的心率、脉搏等信息一起发送给远端的医生,以供医生对病症做出准确诊断,这样更适用于对远端患者疾病的诊断;

[0051] 再次,移动智能终端与医疗收费终端在进行基于NFC的医疗费用支付时,移动智能终端以其构建的人体磁场数据库作为其合法拥有者操作该移动智能终端的身份识别信息,构建其合法拥有者体味数据库以及各手指所对应的静脉信息数据库,以提高移动智能终端认证操作者合法身份的准确性;

[0052] 最后,移动智能终端的合法拥有者以基础颜色为基础,设置其关于费用支付的二次确认支付密码,并生成在预设时间段有效的身份认证密钥,该身份认证密钥是基于该移动智能终端合法拥有者的身份证号码信息中所有数字的累计和值、平均值、身份证号码信息特征值以及第一认证密钥得到,由此提高移动智能终端支付密码的安全性能,防止支付密码被破解,进一步增强移动智能终端对操作者是否具有合法身份的认证准确率,提高了移动智能终端在医疗监护系统处支付医疗费用的安全性能。

附图说明

[0053] 图1为本发明实施例中基于移动近场通信的医疗监护系统的结构示意图;

[0054] 图2为图1所示医疗监护系统中医疗监护床的功能模块连接示意图。

具体实施方式

[0055] 以下结合附图实施例对本发明作进一步详细描述。

[0056] 参见图1和图2所示,本实施例中基于移动近场通信的医疗监护系统,包括移动智能终端1、移动运营商2、认证机构3、医疗监护子系统4、第一银行系统5和第二银行系统6;其中:

[0057] 移动智能终端1包括微处理器100及分别连接微处理器100的二代身份证扫描器101、触摸显示模块102、指纹采集器103、手指静脉信息采集器104、人体磁场采集器105、人体体味采集模块106、基础颜色生成模块107、第一空气湿度采集模块108、第一可见光信息转换模块109、可见光发射模块110、加密模块111、视频采集器112、音频采集器113、脉搏传感器114、心率传感器115、血糖采集器116、握力探测器117、存储器118、第一LTE通信模块119、第一蓝牙模块120、第一NFC通信模块121以及能够检测空闲频段的第一频谱感知模块122,二代身份证扫描器101、指纹采集器103、手指静脉信息采集器104分别连接加密模块111,视频采集器112、音频采集器113、脉搏传感器114、心率传感器115、血糖采集器116和握力探测器117分别连接存储器118;存储器118分别连接第一LTE通信模块119、第一蓝牙模块120和第一NFC通信模块121,视频采集器112、音频采集器113、脉搏传感器114、心率传感器115、血糖采集器116和握力探测器117分别连接第一LTE通信模块119,第一LTE通信模块119连接第一频谱感知模块122;其中:

[0058] 二代身份证扫描器101,用以获取患者的身份证号码信息,并经加密模块111加密后保存到存储器118;指纹采集器103,用以采集移动智能终端1合法拥有者的指纹信息,以确认移动智能终端1利用第一NFC通信模块121完成支付交易的过程;视频采集器112、音频采集器113,用于分别对应获取患者的视频、音频信息,并在保存到存储器118中的同时,利用第一LTE通信模块119传送至医疗监护子系统4,以将患者的音视频信息提供给医生诊断;基础颜色生成模块107,用于生成包括红色、橙色、黄色、绿色、青色、蓝色和紫色的七种基础颜色,并在触摸显示模块102上进行显示,以供用户选择任意的颜色组合作为支付色;第一可见光信息转换模块109,用以将数字信息转换为可见光后,以可见光形式发送出去,从而利用可见光形式保证被传送信息的安全;人体磁场采集器105,用以检测人体磁场数据,并发送检测到的人体磁场数据给微处理器100,以得到作为身份识别特征信息的人体磁场数据库;人体体味采集模块106,用以采集作为身份识别特征信息的人体体味数据,并发送检测到的人体体味数据给微处理器100;第一频谱感知模块122,检测移动智能终端所处通信环境的空闲频段,由微处理器100命令第一LTE通信模块119切换至空闲频段上,以对外发送包括音视频的数据;

[0059] 医疗监护子系统4包括中央处理器400以及分别连接中央处理器400的医疗信息数据库401、医疗监护床402、病历挂号模块403、触摸式显示屏404、滤噪器405、音频处理器406、振动器407、第二频谱感知模块408、第二LTE通信模块409、第二蓝牙模块410、具有第二NFC通信模块411的医疗收费终端412、M个NFC中继通信模块413和医生用挂诊显示器414,触摸式显示屏404和滤噪器405分别连接第二LTE通信模块409,第二LTE通信模块409连接第二

频谱感知模块408;第二蓝牙模块410、第二NFC通信模块411分别连接病历挂号模块403,病历挂号模块403连接医疗信息数据库401,医疗信息数据库401连接医生用挂诊显示器414,音频处理器406连接振动器407,各NFC中继通信模块413分别连接第二NFC通信模块411,医疗监护床402上设置有连接医疗信息数据库401的监护控制器4020、脑电波采集装置4021、脑电波分析装置4022、脑电波控制装置4023、呼叫按钮4024、身体生理参数采集器4025、监护RFID标签4026、监护参数存储器4027、发光装置4028以及医疗监护床单4029,脑电波采集装置4021连接脑电波分析装置4022,医疗监护床单4029上设置有布料检测器4030和压力传感器阵列4031,身体生理参数采集器4025、监护RFID标签4026和压力传感器阵列4031均连接监控参数存储器4027,压力传感器阵列4031和布料检测器4030均连接监护控制器4020;医疗监护子系统4中所有NFC中继通信模块413的个数 $M \geq 2$;其中:

[0060] 脑电波采集装置4021采集患者的脑电波信号,并发送给脑电波分析装置4022;脑电波分析装置4022将接收的患者的脑电波信号转换成预存的患者控制信号且发送给监护控制器4020,并由监护控制器4020控制医疗监护床402上的其他部件,方便患者得到及时的服务;病历挂号模块403实现患者利用移动智能终端1通过第一蓝牙模块120、第二蓝牙模块410配对通信后与其连接,并将挂号患者的身份证号码信息发送至医疗信息数据库401存储,从而较远距离处提前完成挂号,提高挂号效率;医疗信息数据库401,根据挂号患者信息以及挂号先后的顺序,按照挂号先后顺序发送患者信息给医生用挂诊显示器414;医生用挂诊显示器414显示挂号患者信息,以供医生了解包括姓名、性别和年龄等挂号患者信息;触摸式显示屏404显示所接收患者的远程视频,以供医生根据远程视频掌握患者基本病症情况,以指导患者做出急救措施或者在医疗中心提前做出应急准备;滤噪器405滤除所接收患者脉搏音频中的噪声,将获取的纯净的脉搏音频发送给音频处理器406;音频处理器406放大接收的纯净的脉搏音频,提取放大后的脉搏音频的频率和振幅给中央处理器400;第二频谱感知模块408检测医疗服务子系统4周围处于空闲状态的通信频段,并发送给中央处理器400;中央处理器400,接收到音频处理器406发送的脉搏音频振幅后,命令振动器407按照一定频率和振幅做振动以重构患者脉搏,使医生在远端了解患者真实脉搏情况;根据接收的空闲通信频段值,命令第二LTE通信模块409切换至空闲通信频段上传输;获取具有最优中继性能的NFC中继通信模块作为最佳NFC中继通信模块;第二蓝牙模块410配对连接第一蓝牙模块120,实现患者利用移动智能终端1在蓝牙通信距离内即可及时完成挂号;医疗收费终端412通过最佳NFC中继通信模块以及第二NFC通信模块411、第一NFC通信模块121,完成移动智能终端1与医疗收费终端412的近场通信支付交易过程;其中,移动智能终端1与医疗收费终端412实现近场通信支付交易过程包括如下步骤:

[0061] 步骤1,移动智能终端采集、存储其合法拥有者的身份证号码信息,并在预设的时间段内实时采集其合法拥有者的人体磁场数据,构建其合法拥有者在各预设时间段内的人体磁场数据库,并以构建的人体磁场数据库作为其合法拥有者的身份识别信息;其中,预设的时间段包括第一预设时间段和第二预设时间段,第一预设时间段为06:00至18:00;第二预设时间段为18:00至次日06:00;由于每个人身体所具有的磁场是不同的,人体磁场作为每个人独有的生物特征,其与手指指纹一样,可以作为身份识别的人体生物特征信息。人体磁场数据强度在各时间段内并非是恒定不变的,因此,在本实施例,针对人体磁场数据情况预先设置两个时间段,即预设的时间段包括第一预设时间段和第二预设时间段,第一预

设时间段为06:00至18:00;第二预设时间段为18:00至次日06:00;

[0062] 步骤2,移动智能终端采集其合法拥有者的体味数据、接收其合法拥有者的各手指所对应的指纹信息和静脉信息,构建移动智能终端合法拥有者体味数据库以及各手指所对应的指纹信息数据库和静脉信息数据库;移动智能终端分别赋予其合法拥有者的人体磁场具有身份识别的第一优先级、体味数据具有身份识别的第二优先级;在识别操作者是否具有合法身份过程中,第一优先级具有比第二优先级更高的识别可信度;其中,由于每个人的体味是不一样的,人体体味数据同人体磁场、指纹、面部和虹膜等生物特征一样,也具有独特的不可复制性,因此人体的体味数据同样可以用来作为身份识别的特征信息;关于人体磁场和体味数据在识别时的优先级问题,例如,当移动智能终端判断获取的操作者的人体磁场属于其合法拥有者的磁场数据,且判断获取的体味数据不属于其合法拥有者的体味数据时,移动智能终端判断操作者为其合法拥有者;

[0063] 步骤3,移动智能终端在其触摸显示屏上显示预设个数的支付密码输入框给其合法拥有者,各支付密码输入框均分别对应着七种供任意选择的基础颜色列表;其中,基础颜色列表中的七种基础颜色分别为红色、橙色、黄色、绿色、青色、蓝色和紫色,每个支付密码输入框对应着一组支付允许色;各组支付允许色为七种基础颜色的任意组合;例如,移动智能终端在其触摸显示屏上显示3个支付密码输入框,3个支付密码输入框分别编号01输入框、02输入框和03输入框;其中:

[0064] 在01输入框中对应着红色、橙色、黄色、绿色、青色、蓝色和紫色七种基础颜色,

[0065] 在02输入框中对应着红色、橙色、黄色、绿色、青色、蓝色和紫色七种基础颜色,

[0066] 在03输入框中对应着红色、橙色、黄色、绿色、青色、蓝色和紫色七种基础颜色;

[0067] 上述3个支付密码输入框中所提供的基础颜色是相同的,该移动智能终端的合法拥有者在01输入框中可以至少选择一种基础颜色作为该01输入框对应的一组支付允许色,比如说,单独选择红色作为一组支付允许色,也可以选择红色、橙色和黄色这三种基础颜色的组合作为该01输入框对应的一组支付允许色;同样地,02输入框及03输入框中也可以根据需要进行选择设置,以形成各自对应的支付允许色;例如,01输入框对应的一组支付允许色为红色、红色和黄色,02输入框对应的一组支付允许色为橙色和黄色,03输入框对应的一组支付允许色为蓝色和紫色。

[0068] 步骤4,根据触摸显示屏上各支付密码输入框对应的基础颜色列表,移动智能终端的合法拥有者依次选取自定义种类数的基础颜色组合分别作为各支付密码输入框的支付允许色,并由移动智能终端分别对应地存储各支付密码输入框所对应的支付允许色;移动智能终端的合法拥有者在每个支付密码输入框中对应输入的各组支付允许色的整体组合即形成该移动智能终端关于支付的二次确认支付密码;例如,在步骤3所举例说明的3个支付密码输入框中,该移动智能终端的二次确认支付密码为三个输入框所对应各组支付允许色的整体组合,即移动智能终端的二次确认支付密码为“红色、红色、黄色;橙色、黄色;蓝色、紫色”。

[0069] 另外,作为一种更加安全的支付防护方法,移动智能终端的二次确认支付密码为其合法拥有者在每个支付密码输入框中按照先后顺序依次对应输入的各组支付允许色的整体组合;也就是说,各种基础颜色的先后顺序也对二次确认支付密码的设定具有限定作用,即便各组支付允许色中选择的基础颜色一致,但是只要基础颜色输入的先后顺序不对,

则同样不能通过移动智能终端关于二次确认支付密码的认证；例如，移动智能终端的合法拥有者自己设定的二次确认支付密码为“红色、红色、黄色；橙色、黄色；蓝色、紫色”，如果有人，包括该移动智能终端的合法拥有者，输入的二次确认支付密码为“红色、黄色、红色；橙色、黄色；蓝色、紫色”，则该人员仍旧不能通过移动智能终端的安全支付认证，移动智能终端不会开启支付响应，这样可以有效地保证移动智能终端的支付密码信息；

[0070] 由于各支付密码输入框中所对应的每组支付允许色为该移动智能终端的合法拥有者自己设置的，且每组支付允许色中的颜色为移动智能终端的合法拥有者任意随机设置的，因此最终的支付允许色只有该移动智能终端的合法拥有者知悉，其他人员是难以猜测或破解得到正确的支付允许色的，由此提高了移动智能终端的二次确认支付密码的安全性，也增强了移动智能终端对其操作人员是否具有合法身份的认证准确率；

[0071] 步骤5，移动智能终端根据其合法拥有者的身份证号码信息以及关于支付的二次确认支付密码，生成表征移动智能终端合法拥有者对该移动智能终端合法拥有认证信息的身份认证秘钥；其中，身份认证秘钥标记为K，身份认证秘钥K的获取过程包括步骤5-1至步骤5-5：

[0072] 步骤5-1，移动智能终端提取其合法拥有者的身份证号码信息，并分别获取其身份证号码信息中所有数字的身份证号码信息的累计和值、身份证号码信息的平均值以及身份证号码信息特征值；其中：

$$[0073] \quad X = \sum_{i=1}^m x_i, \quad Y = \frac{1}{m} \sum_{i=1}^m x_i, \quad Z = \frac{X}{Y};$$

[0074] X为身份证号码信息的累计和值，Y为身份证号码信息的平均值，Z为身份证号码信息特征值； x_i 为身份证号码中的第i个数字，m为身份证号码信息中所有数字的个数；例如，移动智能终端所对应合法拥有者张三的18位身份证号码信息包括17位数字以及一个字母X，则上述信息中对应的 $m=17$ ；由于每个人的身份证号码信息是唯一的，则在该步骤计算得到的累积和值、身份证号码信息平均值以及身份证号码信息特征值也是唯一的，从而可以利用所得各对应数值作为身份识别的特征值，避免其他非法人员伪造身份信息，以非法方式操作移动智能终端的支付程序；

[0075] 步骤5-2，根据得到的身份证号码信息的累计和值、平均值以及身份证号码信息特征值，得到在预设时间段内有效的第一认证秘钥值；第一认证秘钥值标记为k，第一认证秘钥值k由如下公式得到： $k^3 = Xt^2 + Yt + Z$ ； $t \in (T_1, T_2)$ ；其中，t为移动智能终端的合法拥有者输入完毕二次确认支付密码的时刻， T_1 为身份认证秘钥的预设时间段的起始时刻， T_2 为身份认证秘钥的预设时间段的终止时刻；此处通过设置身份认证秘钥的预设时间段起始时刻和终止时刻，可以使得最终生成的身份认证秘钥受到预设有效时间段的限制，一旦超过了预设的有效时间段，则该身份认证秘钥即使正确，移动智能终端也不认可操作者的合法身份，以此再次确保移动智能终端的二次确认支付密码的安全，杜绝非安全、非合法人员操作移动智能终端的支付程序；

[0076] 步骤5-3，移动智能终端提取各支付密码输入框中对应的每组支付允许色，并计算得到各支付密码输入框中对应每组支付允许色的灰度平均值；其中，各支付密码输入框对

应的一组支付允许色的灰度平均值 $I(n)$ 由如下公式得到：
$$I(n) = \frac{1}{J_n} \sum_{j=1}^{J_n} I(n, j);$$

[0077] 其中, $I(n)$ 为第 n 个支付密码输入框所对应组的支付允许色的灰度平均值, J_n 为第 n 个支付密码输入框中支付允许色所对应基础颜色的个数, $I(n, j)$ 为第 n 个支付密码输入框中第 j 个基础颜色的灰度值, $1 \leq j \leq J_n$;

[0078] 例如, 移动智能终端显示出了 3 个支付密码输入框, 分别编号为 01 号支付密码输入框、02 号支付密码输入框和 03 号支付密码输入框, 则 $n=3$; 在 01 号支付密码输入框中所对应一组支付允许色为红色、红色和黄色, 在 02 号支付密码输入框中所对应一组支付允许色为橙色和黄色, 在 03 号支付密码输入框中所对应一组支付允许色为蓝色和紫色, 则 $J_1=3$, 即 01 号支付密码输入框中支付允许色所对应基础颜色的个数为 3, $I(1, 1)$ 为 01 号支付密码输入框中第一个红色这个基础颜色所对应的灰度值, $I(1, 2)$ 为 01 号支付密码输入框中第二个红色这个基础颜色所对应的灰度值, $I(1, 3)$ 为 01 号支付密码输入框中第三个黄色这个基础颜色所对应的灰度值, 01 号支付密码输入框对应的一组支付允许色的灰度平均值

$$I(1) = \frac{1}{3}[I(1, 1) + I(1, 2) + I(1, 3)];$$

[0079] 对应地, $I(2, 1)$ 为 02 号支付密码输入框中第一个橙色这个基础颜色所对应的灰度值, $I(2, 2)$ 为 02 号支付密码输入框中黄色这个基础颜色所对应的灰度值, 02 号支付密码输入框对应的一组支付允许色的灰度平均值 $I(2) = \frac{1}{2}[I(2, 1) + I(2, 2)]$; $I(3, 1)$ 为 03 号支付密码输入框中第一个蓝色这个基础颜色所对应的灰度值, $I(3, 2)$ 为 03 号支付密码输入框中紫色这个基础颜色所对应的灰度值, 03 号支付密码输入框对应的一组支付允许色的灰度平均值

$$I(3) = \frac{1}{2}[I(3, 1) + I(3, 2)];$$

[0080] 步骤 5-4, 根据各支付密码输入框对应的一组支付允许色的灰度平均值, 计算所有的支付密码输入框中支付允许色的灰度平均值 I ; 其中:

$$[0081] \quad I = \frac{1}{N} \sum_{n=1}^N I(n);$$

[0082] N 为所有支付密码输入框的个数, $I(n)$ 为第 n 个支付密码输入框所对应的一组支付允许色的灰度平均值; 结合步骤 5-3 中关于 01 号支付密码输入框、02 号支付密码输入框和 03 号支付密码输入框的说明, 所有的支付密码输入框中支付允许色的灰度平均值为

$$I = \frac{1}{3}(I(1) + I(2) + I(3));$$

[0083] 步骤 5-5, 根据得到的第一认证密钥值 k 以及支付允许色灰度平均值 I , 得到在预设时间段内有效的身份认证密钥, 并将该身份认证密钥存储到移动智能终端中; 身份认证密钥标记为 K , 身份认证密钥 K 由如下公式得到: $K^3 = Xt^2 + Yt + I$, $t \in [T_1, T_2]$; t 为移动智能终端的合法拥有者输入完毕二次确认支付密码的时刻, T_1 为身份认证密钥的预设时间段的起始时刻, T_2 为身份认证密钥的预设时间段的终止时刻;

[0084] 此步骤的身份认证密钥 K 由有效时间段、移动智能终端合法拥有者的身份证号码信息以及所有支付密码输入框中支付允许色的灰度平均值处理得到, 而支付允许色的灰度平均值又是利用移动智能终端合法拥有者自己唯一设置的, 这些参数使得最终得到的该身份认证密钥 K 是唯一的, 操作者如果不是该移动智能终端的合法拥有者, 则该操作者是难以破解获取的, 从而再次保证了移动智能终端对合法人员身份的认证, 以保证移动智能终端

的支付安全；

[0085] 步骤6,移动智能终端发送其第一NFC通信模块的真实身份标识号给认证机构,由认证机构生成移动智能终端交易用的匿名身份标识号;医疗收费终端发送其第二NFC通信模块的真实身份标识号给认证机构,由认证机构生成医疗收费终端交易用的匿名身份标识号;其中,移动智能终端的真实身份标识号记为 $Mobile_{id}$,认证机构标记为TSM,移动智能终端的匿名身份标识号记为 $Mobile_{aid}$,医疗收费终端的真实身份标识号记为 $Medical_{id}$,医疗收费终端的匿名身份标识号记为 $Medical_{aid}$;

[0086] $Mobile_{aid} = SH(Mobile_{id})$, $Medical_{aid} = SH(Medical_{id})$; $SH(\cdot)$ 为哈希匿名函数,哈希匿名函数为现有技术,此处不作过多赘述;

[0087] 步骤7,移动智能终端在第一银行系统注册其付款账户,医疗监护子系统在第二银行系统注册其收款账户,并作为医疗收费终端的收款账户;其中,移动智能终端的付款账户记为 $Mobile_{acct}$,医疗监护子系统的收款账户记为 $Medical_{acct}$;

[0088] 步骤8,移动智能终端靠近医疗收费终端至近场通信距离以内时,医疗收费终端首先开启近场通信请求,并发送包括可选支付费用清单的支付交易初步认证信息给移动智能终端,用户通过移动智能终端选择所需支付费用名称,然后反馈所需支付费用名称给医疗收费终端,从而开启移动智能终端与医疗收费终端的正式支付交易;

[0089] 步骤9,医疗收费终端根据移动智能终端所需支付费用名称,发送包括对应该费用名称的支付金额、收据单号、医疗收费终端的匿名身份标识号、当前位置空气湿度、收据单号生成时间以及其与认证机构共享秘钥的交易信息给移动智能终端;其中,该交易信息标记为 $E_{Medical}$, $E_{Medical} = E(ReceiptNum, Price, Medical_{aid}, RH_{Medical}, T, K_{Medical-TSM})$;

[0090] $ReceiptNum$ 为医疗收费终端生成的收据单号; $Price$ 为移动智能终端需要支付的金额, $Medical_{aid}$ 为医疗收费终端的匿名身份标识号, $RH_{Medical}$ 为医疗收费终端当前位置空气湿度, T 为收据单号生成时间; $K_{Medical-TSM}$ 为医疗收费终端与认证机构的共享秘钥;医疗收费终端与认证机构两者之间的共享秘钥 $K_{Medical-TSM}$ 只有医疗收费终端、认证机构知悉,其他第三方,包括移动智能终端、非法用户终端均不能获取到该共享秘钥 $K_{Medical-TSM}$,以此保证医疗收费终端的信息安全;医疗收费终端在与移动智能终端交易时,移动智能终端只能获取到医疗收费终端的匿名身份标识号 $Medical_{aid}$,这样可以保证医疗收费终端不会被其他非法第三方冒充进行试图与认证机构、移动智能终端发送支付交易信息,从而保证了医疗收费终端的信息安全;

[0091] 步骤10,医疗收费终端发送包括步骤9中交易信息、医疗监护子系统收款账户以及其与认证机构间的共享秘钥的认证信息给认证结构,移动智能终端发送支付认证信息给认证结构;其中,移动智能终端发送的支付认证信息包括其临时识别码TMSI、其与认证机构间的共享秘钥 $K_{Mobile-TSM}$ 、其位置区识别码LAI、其当前位置空气湿度 RH_{Mobile} 、移动智能终端付款账户 $Mobile_{acct}$ 及医疗收费终端发送的交易信息;移动智能终端发送的支付认证信息记为 E_{Mobile} ;其中:

[0092]
$$E_{Mobile} = E(ReceiptNum, Price, Medical_{aid}, Mobile_{aid}, RH_{Medical}, RH_{Mobile}, T, TMSI, LAI, K_{Mobile-TSM})$$
;

[0093] 步骤11,认证机构提取医疗收费终端所发送信息中的医疗收费终端匿名身份标识号,并基于认证结构中已存储的医疗收费终端真实身份标识号进行匹配判断;

[0094] 当认证机构利用医疗收费终端真实身份标识号以及哈希匿名函数所生成的医疗收费终端匿名身份标识号与提取的医疗收费终端匿名身份标识号匹配一致时,表明发送该认证信息的医疗收费终端可信,则认证机构执行步骤12;否则,认证机构切断与该认证信息所对应医疗收费终端之间的通信,并发送包含此医疗收费终端匿名身份标识号的警告信息给移动智能终端;

[0095] 步骤12,认证机构提取移动智能终端支付认证信息中的临时识别码和位置区识别码,并发送包括移动智能终端临时识别码、位置区识别码以及其与移动运营商间的共享秘钥的反馈认证信息给移动运营商;其中,反馈认证信息记为 E_{MNO} , $E_{MNO} = E(TMSI, LAI, K_{TSM-MNO})$; $K_{TSM-MNO}$ 表示认证机构与移动运营商之间的共享秘钥;

[0096] 步骤13,移动运营商利用其与认证机构间的共享秘钥提取反馈认证信息中的移动智能终端临时识别码和位置区识别码,并根据移动智能终端临时识别码检索得到对应该临时识别码的移动用户识别码后,发送包括移动智能终端临时识别码、位置区识别码以及移动用户识别码的已认证信息给认证机构;

[0097] 步骤14,认证机构提取认证信息中所含有的医疗收费终端当前位置空气湿度以及支付认证信息中所含有的移动智能终端当前位置空气湿度,并判断医疗收费终端当前位置空气湿度与移动智能终端当前位置空气湿度之差低于预设的空气湿度差阈值时,则认证机构发送确认支付命令信息给第一银行系统;其中:所述确认支付命令信息包括需扣除金额、收据单号、收据单号生成时间、移动智能终端支付账户、医疗监护子系统收款账户以及认证机构与第一银行系统间的共享秘钥;确认支付命令信息记为 $E_{Confirm}$,其中:

[0098] $E_{Confirm} = (Amt_{dedt}, ReceiptNum, T, Mobile_{acct}, Medical_{acct}, K_{TSM - BANK_1})$;

[0099] 其中, Amt_{dedt} 为移动智能终端支付账户应扣除的金额, $K_{TSM - BANK_1}$ 为认证机构与第一银行系统间的共享秘钥,第一银行系统标记为 $BANK_1$;医疗收费终端当前位置空气湿度数据,表征了医疗收费终端当前所处环境中的空气环境情况,在同一位置的空气湿度值相同,即在NFC的通信距离内,医疗收费终端与移动智能终端两者获取的当前位置空气湿度数据位于预设的误差范围之内,因此可以利用空气湿度的不可伪装性,即利用同一位置下空气湿度值相同的这一特点来对是否为同一位置进行确定,从而可以进一步确定两者交易行为的安全性;

[0100] 步骤15,第一银行系统根据认证机构所发送的确认支付命令信息以及对应的应扣除金额,在移动智能终端的支付账户中,预扣除对应的金额,并将移动智能终端支付账户中扣除的金额预转移至医疗监护子系统在第二银行系统的收款账户中,并在完成操作后,第一银行系统发送包括扣款金额、扣款时间、银行授权扣款单号、扣款账户、收款账户以及共享秘钥的预扣款回执信息给移动智能终端进行存储,并转至步骤14进行二次支付确认操作;

[0101] 步骤16,移动智能终端采集握持该移动智能终端人员的人体磁场强度、体味数据、指纹信息以及此时的时间值,并对该握持人员的身份进行鉴定判别;

[0102] 当移动智能终端判断此时采集的人体磁场强度存在于移动智能终端已存储的该时间所对应预设时间段内的人体磁场强度数据库,且此时采集的体味数据同样存储于移动智能终端已存储的体味数据库中时,表明该握持人员为移动智能终端的合法拥有者,则移动智能终端执行步骤17;否则,移动智能终端在预设时间段内拒绝该握持人员对移动智能

终端的任何操作；

[0103] 步骤17,移动智能终端在其触摸显示屏显示各支付密码输入框以及对应各支付密码框的基础颜色列表,并在握持人员依次输入各组支付允许后,移动智能终端根据该握持人员输入的各支付密码输入框中的支付允许色进行判断:

[0104] 当各支付密码输入框中的支付允许色与移动智能终端在步骤4中已对应存储的支付允许色完全一致时,表明输入了正确的二次确认支付密码,则移动智能终端执行步骤17;否则,表明输入了错误的二次确认支付密码,则移动智能终端在预设时间段内拒绝该握持人员对移动智能终端的任何操作;

[0105] 步骤18,移动智能终端要求该握持人员输入其身份证号码信息,并基于该握持人员的身份证号码信息生成对应的身份认证密钥 K' ,移动智能终端判断此时生成的身份认证密钥 K' 与其已存储的身份认证密钥 K 一致时,则移动智能终端发送确认转账命令给第一银行系统;否则,移动智能终端在预设时间段内拒绝该握持人员对该移动智能终端的任何关于支付的操作;

[0106] 步骤19,第一银行系统在接收到移动智能终端所发送的支付命令后,第一银行系统转移步骤15中对应的款项给医疗监护子系统的收款账户,并在第二银行系统收到第一银行系统所转移的款项后,发送包括收款金额 Amt_{dedt} 、银行授权收款单号 $BANK_{Trans}$ 、收款账户 $Medical_{acct}$ 和收款时间 T_3 的收款回执信息给医疗监护子系统;收款回执信息标记为 $E_{Receipt}$,其中, $E_{Receipt}=E(Amt_{dedt},BANK_{Trans},Medical_{acct},T_3)$ 。

[0107] 本实施例中,基于移动近场通信的医疗监护系统工作情况如下:

[0108] 当患者需要在医疗监护机构看病时,患者或者其家属利用移动智能终端启动蓝牙功能,并扫描获取患者的二代身份证号码信息,以使移动智能终端连接病历挂号模块,将患者的挂号信息提供至医生用挂诊显示器,同时,移动智能终端还采集患者的脉搏、心率、血糖以及握力等身体特征参数,并也提前发送给医生用挂诊显示器,以方便医生提前了解对应患者的基本病症情况,这样不仅提前全面了解患者基本病症,及时给出有效治疗措施,而且缩减了诊断单个患者病症时间,提高了诊断效率;患者或者其家属需要支付医疗费用时,则利用移动智能终端输入基于支付允许色的支付密码,从而安全地完成费用支付,也减少了排队付费的时间;

[0109] 如果患者不方便去医疗监护机构时,患者利用移动智能终端建立与医疗监护子系统的远程连接,并由移动智能终端发送患者的音视频数据以及脉搏、心率等参数给远端的医生,实现医生远程诊断患者病症的目的;另外,如果患者住院,且不方便活动时,则利用医疗监护床上的各种脑电波装置,完成基本控制,例如,患者利用脑电波控制呼叫按钮启动,还可通过医疗监护床上的压力传感器阵列和监护RFID标签,帮助医生实时了解患者在监护床上的生理参数变化情况,以提出针对措施,帮助患者恢复健康。

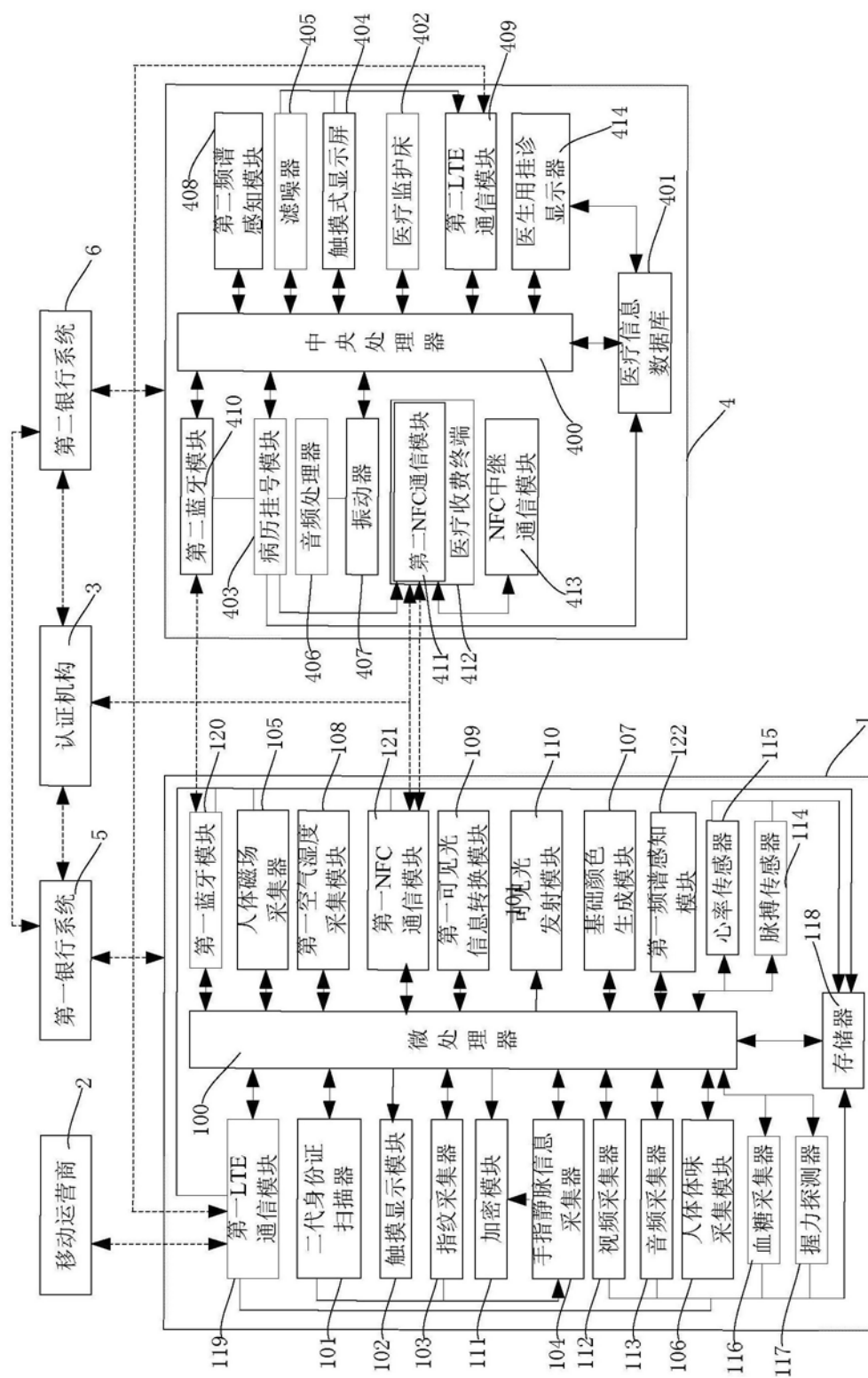


图1

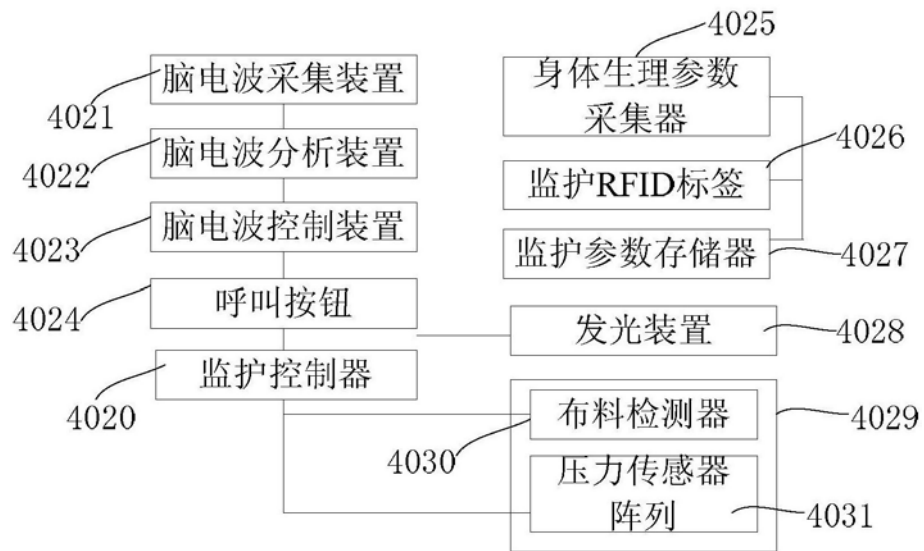


图2

