



(12) 实用新型专利

(10) 授权公告号 CN 205123776 U

(45) 授权公告日 2016. 03. 30

(21) 申请号 201520637084. X

(22) 申请日 2015. 08. 21

(73) 专利权人 广州创弘医疗科技有限公司

地址 510663 广东省广州市萝岗区揽月路 3
号 F113

(72) 发明人 尹洪兵 尹新平

(74) 专利代理机构 北京元中知识产权代理有限
责任公司 11223

代理人 张则武

(51) Int. Cl.

H04L 29/06(2006. 01)

G06K 17/00(2006. 01)

G05B 19/418(2006. 01)

(ESM) 同样的发明创造已同日申请发明专利

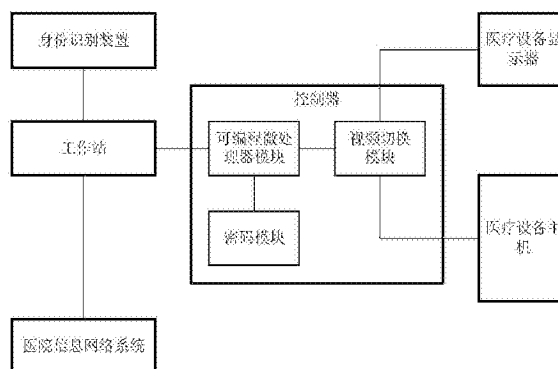
权利要求书1页 说明书9页 附图2页

(54) 实用新型名称

一种医疗设备管理控制系统

(57) 摘要

本实用新型提供一种医疗设备管理控制系统,包括:管理医疗患者在医院的医疗活动信息的医院信息网络系统;获取待使用者的身份信息的身价识别装置;与身价识别装置和医院信息网络系统分别相连的工作站;以及控制器,分别连接有医疗设备显示器和医疗设备主机,与工作站进行数据交互,并根据工作站发送的控制命令控制医疗设备显示器和医疗设备主机的通断。本实用新型可以有效防止医院的私自收费和人情化检查现象,可通过多种途径进行身份认证,并设有加密模块,提高了信息传输的安全性。



1. 一种医疗设备管理控制系统,其特征在于,包括:

管理医疗患者在医院的医疗活动信息的医院信息网络系统;获取待使用者的身份信息的身分识别装置;与身份识别装置和医院信息网络系统分别相连的工作站;以及控制器,分别连接有医疗设备显示器和医疗设备主机,与工作站进行数据交互,并根据工作站发送的控制命令控制医疗设备显示器和医疗设备主机的通断。

2. 根据权利要求1所述的一种医疗设备管理控制系统,其特征在于,所述控制器包括可编程微处理器模块和视频切换模块;

所述可编程微处理器模块分别连接工作站和视频切换模块,所述视频切换模块分别连接医疗设备显示器和医疗设备主机。

3. 根据权利要求2所述的一种医疗设备管理控制系统,其特征在于,所述控制器还包括对工作站和控制器之间的传输数据进行信息保护的密码模块,与可编程微处理器模块相连。

4. 根据权利要求1所述的一种医疗设备管理控制系统,其特征在于,所述身份识别装置包括智能卡读卡器、条码扫描器和磁条卡读卡器中的至少一种。

5. 根据权利要求4所述的一种医疗设备管理控制系统,其特征在于,所述智能卡读卡器可读取接触式智能卡、非接触式智能卡以及身份证中的至少一种;

所述条码扫描器可读取一维码和二维码中的至少一种;

所述磁条卡读卡器至少读取磁条卡。

6. 根据权利要求1所述的一种医疗设备管理控制系统,其特征在于,所述工作站设有主机、显示屏、输入设备和输出设备。

7. 根据权利要求1所述的一种医疗设备管理控制系统,其特征在于,所述工作站安装在台车上,可随台车自由移动。

8. 根据权利要求1所述的一种医疗设备管理控制系统,其特征在于,所述控制器上设有VGA接口、HDMI接口、DVI接口、SDI接口以及DP接口中的至少一种。

一种医疗设备管理控制系统

技术领域

[0001] 本实用新型涉及医疗技术领域,尤其是一种医疗设备管理控制系统。

背景技术

[0002] 目前,我国医疗资源不足且分布不均衡,导致大中型医院人满为患。客观上存在的人情化检查和私自收费检查,极大的影响了医院的运作效率和经济效益。医院中利用医疗设备给病人检查和治疗的机会,具体的科室或者相关的操作人员乱收费时,会加重患者负担的现象在现在社会是普遍存在的,这一方面也加重了医患之间的矛盾,也败坏了医院中的风气。尽管医院在管理上投入了巨大的人力和物力,仍不能从根本上解决这一问题。

[0003] 针对此,CN201420686300.5公开了一种医疗设备漏费控制装置。该装置通过身份证读卡器将身份证信息传给计算机,计算机将身份证信息发给漏费控制器,漏费控制器对身份证信息核对后,接通医疗设备,从而可以进行正常的医疗检查,同时身份证读卡器、计算机、漏费控制器将此次检查全部传送给控费终端机,以便于日后进行查询统计。控费终端机记录患者检查更直接,更简单,更加自动化的方式,降低了医院漏费控制的成本,同时有效的对医院漏费进行控制。

[0004] CN201420658561.6公开了方便查询的医疗设备漏费控制装置。该装置通过身份证读卡器将身份证信息传给计算机,计算机将身份证信息发给漏费控制器,漏费控制器对身份证信息核对后,通过报警器接通医疗设备,从而可以进行正常的医疗检查,同时身份证读卡器、计算机、漏费控制器将此次检查全部传送给控费终端机,以便于日后进行查询统计。控费终端机记录患者检查更直接,更简单,更加自动化的方式,降低了医院漏费控制的成本,同时有效的对医院漏费进行控制。患者能够通过显示屏准确地掌握各项收费的规定价格标准,能够对多项收费进行核对,很好地满足了患者的需求,也减轻了医院财务人员的负担。

[0005] 上述的两个专利均使用漏费控制器对身份证信息进行核对,操作复杂,然而漏费控制器成本也相对很高。另一方面,使用身份证读卡器进行身份认证,应用面过窄,无法应用于现有的医院普遍使用的智能卡、磁条卡或者条码进行身份认证,且漏费控制器与计算机的连接通道上没有设计信息安全方面的机制,漏费控制器容易受到重放攻击,使得原本不符合使用医疗设备的条件的待使用者变为符合使用医疗设备的条件的待使用者,而且后续通过查询系统检查不出异常,其安全性大大降低。

[0006] 有鉴于此特提出本实用新型。

实用新型内容

[0007] 本实用新型的目的在于克服现有技术的不足,提供一种医疗设备管理控制系统,该管理控制系统加强了医院医疗设备的管理,从而避免私自收费和人情化检查,解决现有医务人员滥用医疗设备医院无法控制的问题。

[0008] 为实现上述目的,本实用新型采用如下技术方案:

[0009] 提供一种医疗设备管理控制系统,包括:管理医疗患者在医院的医疗活动信息的医院信息网络系统;获取待使用者的身份信息、身份识别装置;与身份识别装置和医院信息网络系统分别相连的工作站;以及控制器,分别连接有医疗设备显示器和医疗设备主机,与工作站进行数据交互,并根据工作站发送的控制命令控制医疗设备显示器和医疗设备主机的通断。

[0010] 进一步地,所述控制器包括可编程微处理器模块和视频切换模块;

[0011] 所述可编程微处理器模块分别连接工作站和视频切换模块,所述视频切换模块分别连接医疗设备显示器和医疗设备主机。

[0012] 进一步地,所述控制器还包括对工作站和控制器之间的传输数据进行信息保护的密码模块,与可编程微处理器模块相连。

[0013] 进一步地,所述身份识别装置包括智能卡读卡器、条码扫描器和磁条卡读卡器中的至少一种。

[0014] 进一步地,所述智能卡读卡器可读取接触式智能卡、非接触式智能卡以及身份证中的至少一种;

[0015] 所述条码扫描器可读取一维码和二维码中的至少一种;

[0016] 所述磁条卡读卡器至少读取磁条卡。

[0017] 进一步地,所述工作站设有主机、显示屏、输入设备和输出设备。

[0018] 进一步地,所述工作站安装在台车上,可随台车自由移动。

[0019] 进一步地,所述控制器上设有VGA接口、HDMI接口、DVI接口、SDI接口以及DP接口中的至少一种。

[0020] 采用上述技术方案后,本实用新型与现有技术相比具有如下优点:

[0021] (1)本实用新型的身份认证功能设置在工作站端,可通过多种途径获取待使用者的身份信息,包括通过智能卡读卡器可读取接触式智能卡、非接触式智能卡以及身份证等;通过条码扫描器可读取一维码、二维码等;通过磁条卡读卡器可读取磁条卡等,符合大部分医院在挂号、缴费等方面的身份认证需求;

[0022] (2)本实用新型的工作站直接连接医院信息网络系统,工作站从身份识别装置获取到身份信息后,可立即从医院信息网络系统中获取到与此身份信息对应的医疗活动信息,并根据医院的管理规则实时判断此身份信息是否符合使用医疗设备的条件;

[0023] (3)本实用新型的工作站与控制器之间设有加密机制,数据的传输均为密文,可防止不符合使用医疗设备的条件的待使用者进行重放攻击,提高整个控制系统的安全性;

[0024] (4)对整个系统而言,本实用新型将身份认证功能设计在工作站端,通过智能卡读卡器、条码扫描器或磁条卡读卡器获取待使用者的身份信息,通过身份信息从医院信息网络系统中获取待使用者的其他状态信息,如是否挂号、到科室就诊,是否已经缴纳使用医疗设备所需的费用等,再根据医院的管理规则判断待使用者是否符合使用医疗设备的条件,如果符合,工作站发送指令给控制器,接通医疗设备显示器与医疗设备主机之间的连接。若不符合,则医疗设备主机无法将视频信号传输给医疗设备显示器,从而无法使用,从而可规范化的控制医疗设备的使用。

附图说明

[0025] 为了更清楚地说明本实用新型实施例中的技术方案,下面将对实施例描述中所需要使用的附图作简单地介绍,显而易见地,下面描述中的附图仅仅是本实用新型的一些实施例,对于本领域普通技术人员来讲,在不付出创造性劳动的前提下,还可以根据这些附图获得其他的附图。

[0026] 图1是本实用新型提供的一种医疗设备管理控制系统的结构示意图;

[0027] 图2是本实用新型提供的一种医疗设备管理控制系统的控制方法的流程图。

具体实施方式

[0028] 在本实用新型中,医疗患者指在医院按照医院管理流程进行医疗活动的人,医疗患者在进行某些医疗活动时,需要使用医疗设备进行检查或治疗,为方便表述,本专利中将需要使用医疗设备的医疗患者简称为待使用者。为使本实用新型的目的、技术方案和优点更加清楚,下面将结合附图及具体实施例对本实用新型进一步描述。

[0029] 实施例一

[0030] 如图1所示,本实施例提供一种医疗设备管理控制系统,包括医院信息网络系统、身份识别装置、工作站、控制器、医疗设备显示器以及医疗设备主机;其中,身份识别装置与工作站连接,工作站与控制器和医院信息网络系统分别连接,控制器与医疗设备显示器和医疗设备主机分别连接。

[0031] 医院信息网络系统,管理医疗患者在医院的医疗活动信息,包括医疗患者在医院的挂号、就诊、缴费等,且医院信息网络系统根据医疗患者的医疗活动状态实时更新相关医疗活动信息。其中,医院信息网络系统对工作站开放获取医疗活动信息的权限,用于支持工作站查询待使用者的相关医疗活动信息。

[0032] 身份识别装置,获取待使用者的身份信息。对于不同的医院,其读取待使用者身份信息的方式可能不同,为提高医疗设备管理控制系统的兼容性,该身份识别装置包括智能卡读卡器、条码扫描器和磁条卡读卡器中的至少一种。其中,智能卡读卡器可以读取接触式智能卡、非接触式智能卡以及身份证中的至少一种;条码扫描器可读取一维码和二维码中的至少一种;磁条卡读卡器至少读取磁条卡。当待使用者进行相应读卡或读码后,身份识别装置将待使用者的相关身份信息发送给工作站。

[0033] 工作站,接收身份识别装置发送的身份信息,查询医院信息网络系统中与此身份信息相对应的医疗活动信息并进行判断,根据判断结果向控制器发送相应的控制命令。优选的,工作站设有主机、显示屏、输入设备和输出设备,输入设备优选为键盘和鼠标,输出设备优选为打印机。优选的,工作站设置在台车上,可随台车自由移动。

[0034] 当工作站接收到身份识别装置发送的身份信息时,在医院信息网络系统中查询与该身份信息对应的医疗活动信息,并根据医院的管理规则,判断该身份信息是否符合使用医疗设备的条件。具体地,工作站判断该身份信息对应的医疗活动信息的当前状态是否符合使用医疗设备的条件,如果是,则控制控制器接通医疗设备显示器与医疗设备主机之间的连接;如果否,则在工作站上提示身份信息不符合使用医疗设备的条件。优选的,当工作站判断该身份信息不符合使用医疗设备的条件时,不向控制器发送任何控制命令;进一步优选的,当工作站判断该身份信息不符合使用医疗设备的条件时,向控制器发送断开医疗设备显示器和医疗设备主机连接的控制命令。

[0035] 优选的,使用医疗设备的条件至少包括:与待使用者的身份信息相对应的医疗活动信息的状态为已缴纳使用医疗设备所需的费用。

[0036] 控制器,与工作站进行数据交互,并根据工作站发送的控制命令控制医疗设备显示器和医疗设备主机的通断。

[0037] 其中,控制器包括可编程微处理器模块和视频切换模块,可编程微处理器模块分别连接工作站和视频切换模块,视频切换模块分别连接医疗设备显示器和医疗设备主机。

[0038] 具体地,可编程微处理器模块可根据工作站发送的控制命令向视频切换模块发送相应的视频切换指令;视频切换模块根据可编程微处理器模块发送的视频切换指令控制医疗设备显示器和医疗设备主机的通断。

[0039] 其工作过程为:当工作站判断当前身份信息符合使用医疗设备的条件时,向可编程微处理器模块发送接通医疗设备主机和医疗设备显示器连接的控制命令,可编程微处理器模块收到控制命令后向视频切换模块发送接通医疗设备主机与医疗设备显示器连接的视频切换指令,视频切换模块将医疗设备主机发送的视频信号转送至医疗设备显示器上进行显示,则待使用者可以开始使用医疗设备。

[0040] 进一步地,控制器还包括密码模块,与可编程微处理器模块相连,对工作站和控制器之间的传输数据进行信息保护。

[0041] 其工作过程为:当工作站判断当前身份信息符合使用医疗设备的条件时,工作站向控制器发送获取随机数的请求命令,控制器中的密码模块随机产生一随机数,并通过可编程微处理器模块发送给工作站,工作站将该随机数与自身预设的指令数据进行异或运算后得到第一数据,对第一数据进行加密后得到第一密文,并将第一密文发送至可编程微处理器模块,可编程微处理器模块将第一密文发送给密码模块并指示其对此密文进行解密后得到第一数据,可编程微处理器模块将第一数据与随机数进行异或运算后得到第二数据,并判断第二数据与预设的指令数据是否相同,如果否则向工作站发出指令错误的提示,如果是,则向视频切换模块发送接通医疗设备主机和医疗设备显示器连接的视频切换指令,视频切换模块将医疗设备主机发送的视频信号转送至医疗设备显示器上进行显示,则待使用者可以开始使用医疗设备。

[0042] 其中,可编程微处理器模块和工作站中预设有相同的指令数据,该指令数据并不直接在工作站与控制器之间进行传输,而是参与到数据加密中,因此工作站与控制器之间的数据传输均为密文,且密码模块每次发送的随机数均为随机产生,并参与到数据加密中,如此提高信息传输的安全性。

[0043] 优选的,加密算法为对称加密算法,具体地,在工作站与密码模块中内置有高度保密的对称密钥,加密时工作站使用对称密钥对第一数据进行加密得到第一密文,解密时密码模块使用相同的对称密钥对第一密文进行解密得到第一数据。

[0044] 进一步优选的,加密算法为非对称加密算法,具体地,在工作站中内置有高度保密的非对称密钥中的公钥,在密码模块中内置有高度保密的非对称密钥中的私钥,其中,公钥与私钥相匹配且成对使用,加密时工作站使用非对称密钥中的公钥对第一数据进行加密得到第一密文,解密时密码模块使用非对称密钥中的私钥对第一密文进行解密得到第一数据。

[0045] 其中,医疗设备由医疗设备主机和医疗设备显示器组成,医疗设备为医院中可进

行医疗检查或者治疗的设备,如B超机、内窥镜等。其中,医疗设备主机的视频传输线接入控制器的视频输入端,医疗设备显示器的视频传输线接入控制器的视频输出端,并由控制器的视频切换模块控制二者之间的视频通断。优选的,控制器的输入端/输出端设有VGA接口、HDMI接口、DVI接口、SDI接口以及DP接口中的至少一种,以满足不同设备的连接需求。优选的,连入控制器视频输入端和输出端的视频线使用螺丝固定于控制器中,以防止医院工作人员随意插拔医疗设备的视频线进行人情化检查。

[0046] 使用时先将医疗设备主机和医疗设备显示器的电源接通,待使用者在身份识别装置上刷卡或读码后,工作站判断该身份信息是否符合使用医疗设备的条件,如果符合使用医疗设备的条件,则由控制器控制医疗设备主机和医疗设备显示器接通,待使用者开始使用医疗设备,使用完成后,工作站生成报告,并执行使用完成的操作,工作站指示控制器断开医疗设备主机和医疗设备显示器之间的连接,同时工作站将此次使用所产生的结果、使用的开始时间、结束时间以及持续时间中的至少一种上传至医院信息网络系统进行保存。

[0047] 优选的,在本实施例中,控制器还可设置电源控制模块,接线时将医疗设备主机和医疗设备显示器的电源线接入到控制器中,由控制器中的电源控制模块根据可编程微处理器模块发送的控制指令直接控制医疗设备主机和医疗设备显示器的电源的通断,进一步加强对医疗设备的控制,防止私自收费和人情化检查的发生。

[0048] 本实施例中的身份识别装置可以兼容多种身份认证方式,且工作站与医院信息网络系统直接连接,可以实时获取待使用者的医疗活动状态,工作站安装在台车上可自由移动,控制器与医疗设备主机和医疗设备显示器分别连接,可有效避免医院私自收费和人情化检查的现状,且工作站中设有密码模块,提高了工作站与控制器之间数据传输的安全性,防止不法人员的重放攻击,保证信息安全。

[0049] 实施例二

[0050] 如图2所示,本实施例提供一种医疗设备管理控制系统的控制方法,该医疗设备管理控制系统包括工作站,分别连接有身份识别装置、医院信息网络系统以及控制器,控制器包括可编程微处理器模块,分别连接工作站、密码模块和视频切换模块,视频切换模块分别连接有医疗设备显示器和医疗设备主机,其控制方法包括:

[0051] 步骤101:通过身份识别装置获取待使用者的身份信息并发送至工作站。

[0052] 其中,对于不同的医院,其读取待使用者身份信息的方式可能不同,为提高医疗设备管理控制系统的兼容性,该身份识别装置包括智能卡读卡器、条码扫描器和磁条卡读卡器中的至少一种。其中,智能卡读卡器可以读取接触式智能卡、非接触式智能卡以及身份证中的至少一种;条码扫描器可读取一维码和二维码中的至少一种;磁条卡读卡器至少读取磁条卡。

[0053] 当待使用者请求使用医疗设备时,需要进行相应读卡或读码,身份识别装置获取该身份信息并发送至工作站。

[0054] 例如,对于某医院使用身份证进行身份认证,待使用者A需要使用的医疗设备为B超机,在使用B超机之前,需要在身份识别装置上读取身份证A,身份识别装置获取身份信息A后发送至工作站。

[0055] 特别的,医疗设备在使用之前,医疗设备主机与医疗设备显示器处于断开状态。

[0056] 步骤102:工作站根据接收到的身份信息,查询医院信息网络系统中与该身份信息

相对应的医疗活动信息。

[0057] 医院信息网络系统,管理医疗患者在医院的医疗活动信息,包括医疗患者在医院的挂号、就诊、缴费、是否已经完成使用医疗设备等,且医院信息网络系统根据医疗患者的医疗活动状态实时更新相关医疗活动信息。其中,医院信息网络系统对工作站开放获取医疗活动信息的权限,用于支持工作站查询待使用者的相关医疗活动信息。

[0058] 例如,进行B超检查的待使用者在进行检查之前,待使用者使用身份证A在医院进行了挂号、就诊以及需要进行B超检查,并缴纳了相关费用,这一系列医疗活动被记录在医院信息网络系统中且与待使用者的身份信息A相对应,工作站接收到待使用者的身份信息A后,查询医院信息网络系统中该身份信息A对应的医疗活动信息,其医疗活动信息如表1所示。

[0059]

身份信息		医疗活动	缴费(元)	状态
姓名	王某某	挂号	5	
性别	女	就诊	0	
身份证 A	身份信息 A	B 超检查	100	未检查

[0060] 表1

[0061] 步骤103:工作站判断该身份信息是否符合使用医疗设备的条件。

[0062] 具体地,工作站根据医院的管理规则判断该身份信息对应的医疗活动信息的当前状态是否符合使用医疗设备的条件;若是则执行步骤104;若否则提示该身份信息不符合使用医疗设备的条件。

[0063] 优选的,使用医疗设备的条件至少包括:与待使用者的身份信息相对应的医疗活动信息的状态为已缴纳使用医疗设备所需的费用。

[0064] 例如,医院对B超机使用的管理规则为:缴纳B超检查的费用且未进行检查时即可使用B超机,对于如表1所示的身份信息A对应的医疗活动信息,使用B超检查所需的费用已缴纳,检查状态为未检查,则工作站判断该身份信息符合使用医疗设备的条件。

[0065] 优选的,在判断身份信息是否符合使用医疗设备的条件后,还记录本次判断结果,并发送给医院信息网络系统保存,作为该待使用者的一个状态。

[0066] 优选的,当工作站判断该身份信息不符合使用医疗设备的条件时,不向控制器发送任何控制命令;进一步优选的,当工作站判断该身份信息不符合使用医疗设备的条件时,向控制器发送断开医疗设备显示器和医疗设备主机连接的控制命令。

[0067] 步骤104:工作站向控制器发送获取随机数的请求命令,控制器随机生成一随机数并发送给工作站。

[0068] 具体地,工作站向控制器中的可编程微处理器模块发送获取随机数的请求命令,可编程微处理模块向密码模块发送获取随机数的请求指令,密码模块收到指令后随机生成一随机数,并将该随机数发送至可编程微处理器模块,可编程微处理器保存后将随机数发

给工作站。

[0069] 步骤105:工作站将随机数与预设的指令数据进行第一数学运算后得到第一数据。

[0070] 其中,工作站和可编程微处理器模块中预设有相同的指令数据,该指令数据用于指示接通医疗设备主机和医疗设备显示器的连接,并不直接在工作站与控制器之间进行传输,而是参与到数据加密中,因此工作站与控制器之间的数据传输均为密文,且密码模块每次发送的随机数均为随机产生,并参与到数据加密中,如此提高信息传输的安全性。

[0071] 优选的,密码模块产生的随机数长度与指令数据的长度相同;优选的,第一数学运算为异或运算,可代替的运算还包括加法运算或减法运算等。

[0072] 例如,工作站和可编程微处理器模块中预设的指令数据为Y(0101),随机数为R(1101),则随机数R与指令数据Y进行异或运算后得到第一数据B(1000)。

[0073] 步骤106:工作站对第一数据进行加密后得到第一密文,并将第一密文发送至控制器中的可编程微处理器模块。

[0074] 优选的,加密算法为对称加密算法,具体地,在工作站与密码模块中内置有高度保密的对称密钥,加密时工作站使用对称密钥对第一数据进行加密得到第一密文,解密时密码模块使用相同的对称密钥对第一密文进行解密即可得到第一数据。

[0075] 例如,工作站使用内置的对称密钥K对第一数据B(1000)进行加密后得到第一密文X,并将第一密文X发送至控制器中的可编程微处理器模块。

[0076] 进一步优选的,加密算法为非对称加密算法,具体地,在工作站中内置有高度保密的非对称密钥中的公钥,在密码模块中内置有高度保密的非对称密钥中的私钥,公钥与私钥相匹配且成对使用,加密时工作站使用非对称密钥中的公钥对第一数据进行加密得到第一密文,解密时密码模块使用非对称密钥中的私钥对第一密文进行解密即可得到第一数据。

[0077] 例如,工作站使用内置的公钥PubK对第一数据B(1000)进行加密后得到第一密文E,并将第一密文E发送至控制器中的可编程微处理器模块。

[0078] 步骤107:密码模块对第一密文进行解密后得到第一数据。

[0079] 具体地,可编程微处理器模块接收到第一密文后发送至密码模块,密码模块对第一密文进行解密。

[0080] 优选的,加密算法为对称加密算法时,密码模块使用内置的对称密钥对第一密文进行解密后得到第一数据。例如,对于第一密文X,密码模块使用内置的对称密钥K对第一密文X进行解密,得到第一数据B(1000)。

[0081] 进一步优选的,加密算法为非对称加密算法时,密码模块使用内置的私钥数据对第一密文进行解密后得到第一数据。例如,对于第一密文E,密码模块使用内置的私钥PriK对第一密文E进行解密,得到第一数据B(1000)。

[0082] 步骤108:可编程微处理器模块将第一数据与随机数进行第二数学运算后得到第二数据。

[0083] 其中,第二数学运算与第一数学运算相对应,当第一数学运算为异或运算时,第二数学运算也为异或运算;当第一数学运算为加法运算时,第二数学运算为减法运算;当第一数学运算为减法运算时,第二数学运算为加法运算;优选的,第二数学运算为异或运算。

[0084] 具体地,密码模块将解密后的第一数据发送给可编程微处理器模块,可编程微处

理器模块将第一数据与随机数进行异或运算后得到第二数据。

[0085] 例如,密码模块将解密后的第一数据B(1000)发送给可编程微处理器模块,可编程微处理器模块将第一数据B(1000)与随机数R(1101)进行异或运算后得到第二数据D(0101)。

[0086] 步骤109:可编程微处理器模块判断第二数据与预设的指令数据是否相同,如果是则执行步骤110,如果否则向工作站发出指令错误的提示。

[0087] 其中,该预设的指令数据与工作站中预设的指令数据相同,该指令数据用于指示接通医疗设备主机和医疗设备显示器的连接,并不直接在工作站与控制器之间进行传输,而是参与到数据加密中,提高信息传输的安全性。

[0088] 例如,对于预设的指令数据Y(0101),其第二数据为D(0101),可编程微处理器模块的判断结果为二者相同。

[0089] 优选的,当可编程微处理器模块向工作站发送指令错误的提示时,不向视频切换模块发送任何指令;进一步优选的,当可编程微处理器模块向工作站发送指令错误的提示时,向视频切换模块发送断开医疗设备主机和医疗设备显示器连接的指令。

[0090] 步骤110:可编程微处理器模块向视频切换模块发送接通医疗设备主机和医疗设备显示器连接的视频切换指令。

[0091] 步骤111:视频切换模块接通医疗设备主机和医疗设备显示器之间的连接。

[0092] 具体地,视频切换模块将医疗设备主机发送的视频信号转送至医疗设备显示器。

[0093] 其中,医疗设备由医疗设备主机和医疗设备显示器组成,医疗设备为医院中可进行医疗检查或者治疗的设备,如B超机、内窥镜等。其中,医疗设备主机的视频传输线接入控制器的视频输入端,医疗设备显示器的视频传输线接入控制器的视频输出端,并由控制器的视频切换模块控制二者之间的视频通断。优选的,控制器的输入端/输出端设有VGA接口、HDMI接口、DVI接口、SDI接口以及DP接口中的至少一种,以满足不同设备的连接需求。

[0094] 步骤112:使用完成后,工作站生成报告和本次使用的日志信息,并发送给医院信息网络系统保存,并将指示此待使用者已经完成使用的标识发送给医院信息网络系统保存,同时向控制器发送断开医疗设备主机与医疗设备显示器连接的控制命令。

[0095] 具体地,工作站向可编程微处理器模块发送断开医疗设备主机与医疗设备显示器连接的控制命令,可编程微处理器模块向视频切换模块发送断开医疗设备主机与医疗设备显示器连接的控制指令,视频切换模块断开医疗设备主机与医疗设备显示器之间的连接,恢复到初始状态。

[0096] 其中,日志信息记录了本次使用的所有信息,包括待使用者的身份信息、该身份信息是否符合使用医疗设备的条件、使用的开始时间、结束时间、持续时间、所在医疗科室以及医疗设备型号中的至少一种。

[0097] 其中,报告还可在工作站上进行打印,向病人出示本次使用结果的具体情况,优选的,报告包括以下信息中的至少一种:待使用者的身份信息、此次使用所产生的结果、对结果的具体分析以及给出的处理方案等。

[0098] 本实施例中的医疗设备管理控制系统的控制方法,采用多样化的身份信息获取方式,提高了系统的兼容性,且在工作站和控制器之间的数据传输均为密文,利用密码模块产生随机数并参与到数据加密中,提高了数据传输的安全性,并使用对称加密算法/非对称加

密算法对数据进行二次加密,进一步提高了数据传输的安全性,且利用视频切换模块根据控制指令控制医疗设备显示器和医疗设备的接通和断开,有效地杜绝了医院中的私自收费和人情化检查的现状,成本低,操作简单,适合大量推广。

[0099] 上述实施例中的实施方案可以进一步组合或者替换,且实施例仅仅是对本实用新型的优选实施例进行描述,并非对本实用新型的构思和范围进行限定,在不脱离本实用新型设计思想的前提下,本领域中专业技术人员对本实用新型的技术方案做出的各种变化和改进,均属于本实用新型的保护范围。

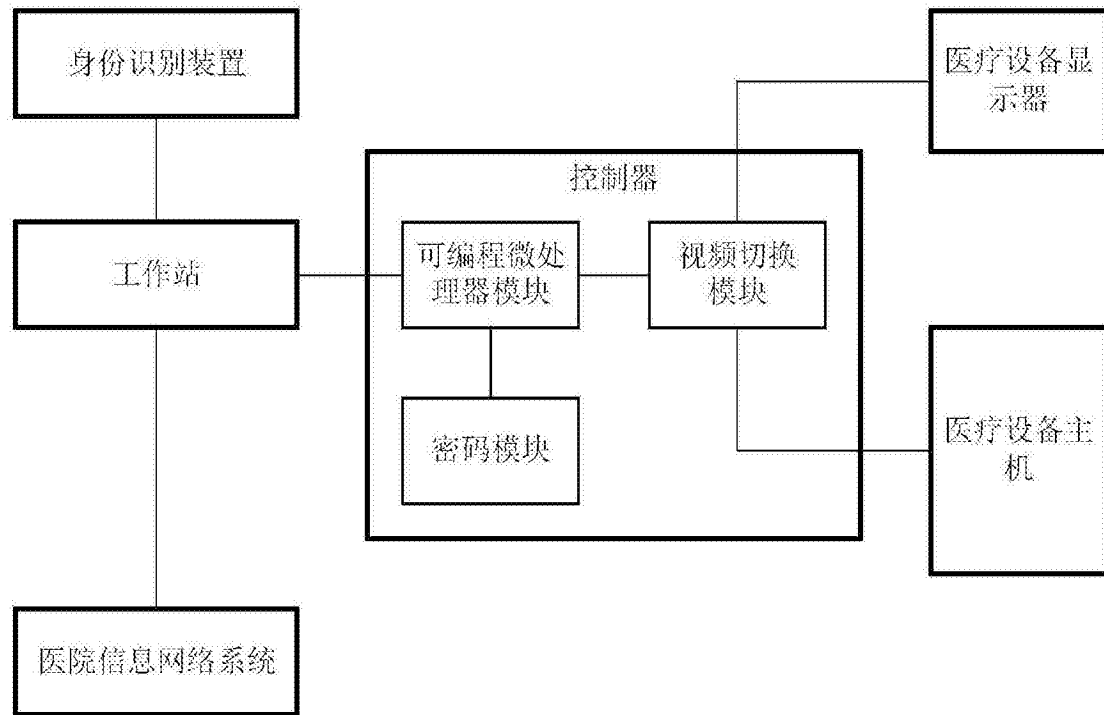


图1

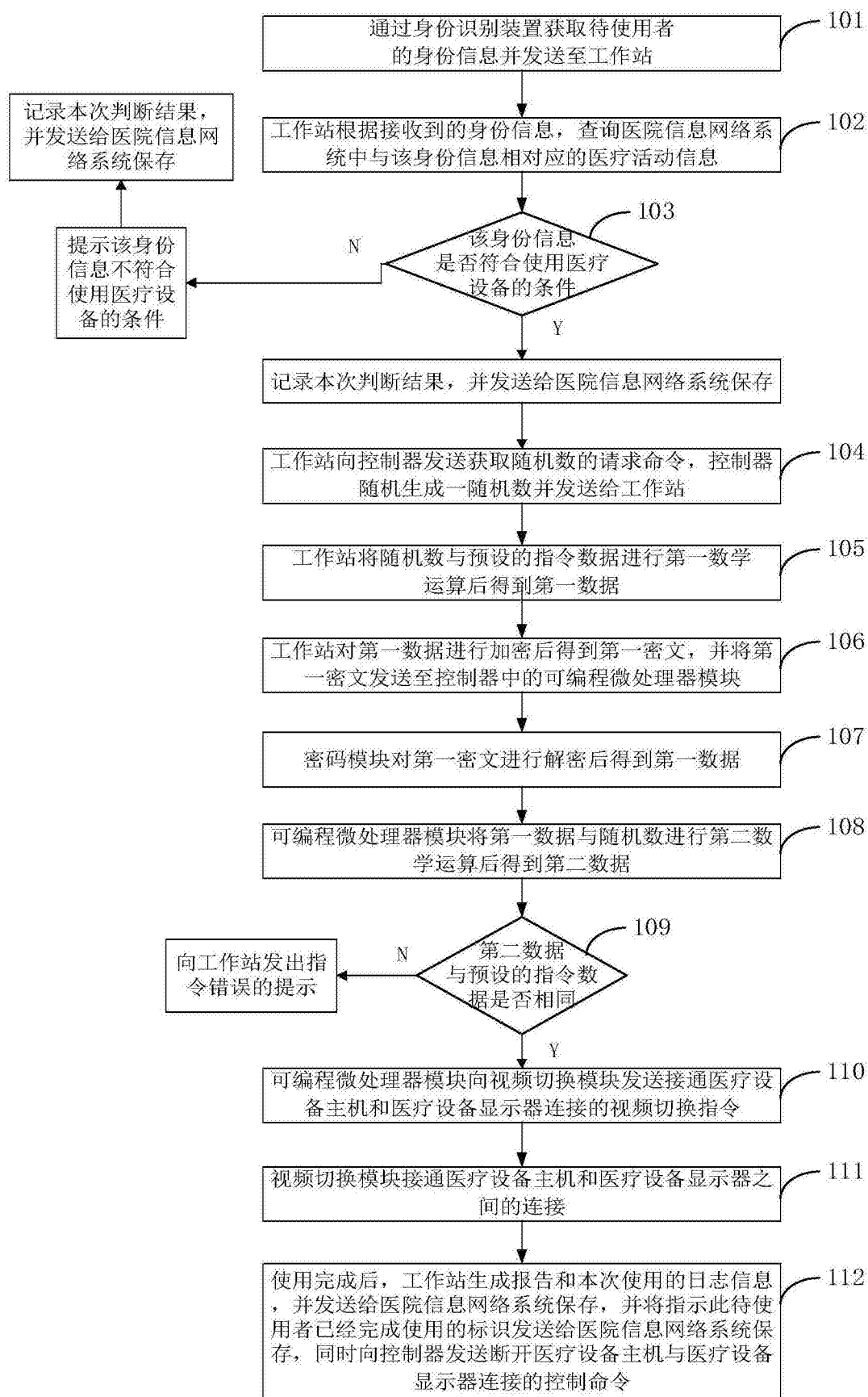


图2