(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 107067056 A
(43)申请公布日 2017.08.18

(21)申请号 201710078901.6

(22)申请日 2017.02.14

(71)申请人 阿里巴巴集团控股有限公司
地址 英属开曼群岛大开曼资本大厦一座四层847号邮箱

(72)发明人 郭伟

(74)专利代理机构 北京国昊天诚知识产权代理有限公司 11315
代理人 黄熊

(51)Int.Cl.
G06K 17/00(2006.01)
G06K 19/06(2006.01)
H04L 9/32(2006.01)

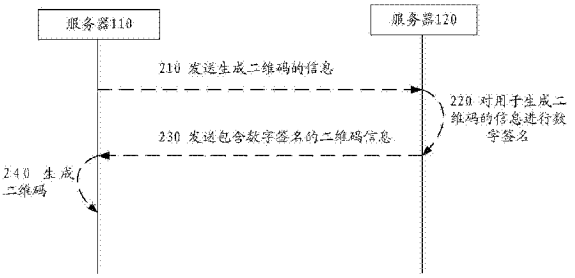
权利要求书3页 说明书10页 附图6页

(54)发明名称

二维码生成方法及其设备和二维码识别方法及其设备

(57)摘要

本申请公开了一种二维码生成方法及其设备和二维码识别方法及其设备。所述方法包括：第一服务器向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息；第二服务器根据接收到的生成二维码的请求，对用于生成二维码的信息进行数字签名；将包含有数字签名的二维码信息发送到第一服务器；第一服务器利用所述二维码信息，生成二维码。根据本发明的实施例通过一服务器与另一服务器之间协同作用产生二维码，增强了二维码的安全性和有效性，并且方便在二维码识别过程中识别出二维码是否被篡改。



CN 107067056 A

1.一种二维码生成方法,其特征在于,包括:

第一服务器向第二服务器发送生成二维码的请求,所述请求包括用于生成二维码的信息;

第二服务器根据接收到的生成二维码的请求,对用于生成二维码的信息进行数字签名;

将包含有数字签名的二维码信息发送到第一服务器;

第一服务器利用所述二维码信息,生成二维码。

2.如权利要求1所述的方法,其特征在于,第一服务器向第二服务器发送生成二维码的请求之前还包括:第一服务器向第二服务器发送注册请求,所述注册请求包括与本次注册相关的所有信息。

3.如权利要求2所述的方法,其特征在于,在第一服务器向第二服务器发送注册请求之后还包括:第二服务器根据所述注册请求,完成对第一服务器的注册。

4.如权利要求3所述的方法,其特征在于,第二服务器根据接收到的生成二维码的请求对用于生成二维码的信息进行数字签名之前还包括:

确定第一服务器是否向第二服务器注册;

若是,则第二服务器根据接收到的生成二维码的请求对用于生成二维码的信息进行数字签名;

若否,则第二服务器不执行对用于生成二维码的信息进行数字签名并向第一服务器发送注册邀请。

5.如权利要求1至4中的任一权利要求所述的方法,其特征在于,第二服务器根据接收到的生成二维码的请求对用于生成二维码的信息进行数字签名的步骤包括:第二服务器在接收到生成二维码的请求之后,基于非对称加密算法,利用私钥对用于生成二维码的信息进行数字签名。

6.如权利要求5所述的方法,其特征在于,根据生成二维码的信息的不同,在对用于生成二维码的信息进行数字签名的步骤中使用的私钥不同。

7.一种二维码生成方法,所述方法由第一服务器执行,其特征在于,包括:

向第二服务器发送生成二维码的请求,所述请求包括用于生成二维码的信息;

从第二服务器接收由第二服务器生成的包含有数字签名的二维码信息;

利用所述二维码信息,生成二维码。

8.如权利要求7所述的方法,其特征在于,向第二服务器发送生成二维码的请求之前还包括:向第二服务器发送注册请求,所述注册请求包括与本次注册相关的所有信息。

9.一种二维码生成设备,其特征在于,包括:

发送单元,向第二服务器发送生成二维码的请求,所述请求包括用于生成二维码的信息;

接收单元,从第二服务器接收由第二服务器生成的包含有数字签名的二维码信息;

生成单元,利用所述二维码信息,生成二维码。

10.如权利要求9所述的设备,其特征在于,其特征在,发送单元在向第一服务器发送生成二维码的请求之前,向第一服务器发送注册请求,所述注册请求包括与本次注册相关的所有信息。

11.一种二维码生成方法，所述方法由第二服务器执行，其特征在于，包括：

从第一服务器接收生成二维码的请求，所述请求包括用于生成二维码的信息；

对用于生成二维码的信息进行数字签名；

将包含有数字签名的二维码信息发送到第一服务器。

12.如权利要求11所述的方法，其特征在于，在从第一服务器接收生成二维码的请求之前还包括：从第一服务器接收注册请求，所述注册请求包括与本次注册相关的所有信息。

13.如权利要求12所述的方法，其特征在于，在从第一服务器接收到注册请求之后，还包括：根据所述注册请求，完成对第一服务器的注册。

14.如权利要求13所述的方法，其特征在于，在对用于生成二维码的信息进行数字签名之前还包括：

确定第一服务器是否在第二服务器中注册：

若是，则根据接收到的生成二维码的请求对用于生成二维码的信息进行数字签名；

若否，则不执行对用于生成二维码的信息进行数字签名并向第一服务器发送注册邀请。

15.如权利要求11至14中的任一权利要求所述的方法，其特征在于，对用于生成二维码的信息进行数字签名的步骤包括：基于非对称加密算法，利用私钥对用于生成二维码的信息进行数字签名。

16.如权利要求15所述的方法，其特征在于，根据生成二维码的信息的不同，在对用于生成二维码的信息进行数字签名的步骤中使用的私钥不同。

17.一种二维码生成装置，其特征在于，包括：

接收单元，从第一服务器接收生成二维码的请求，所述请求包括用于生成二维码的信息；

处理单元，对用于生成二维码的信息进行数字签名；

发送单元，将包含有数字签名的二维码信息发送到第一服务器。

18.如权利要求17所述的装置，其特征在于，接收单元还从第一服务器接收注册请求，所述注册请求包括与本次注册相关的所有信息。

19.如权利要求18所述的装置，其特征在于，还包括：注册单元，根据所述注册请求，完成对第一服务器的注册。

20.如权利要求19所述的装置，其特征在于，还包括：确定单元确定第一服务器是否在第二服务器中注册：

若是，则根据接收到的生成二维码的请求对用于生成二维码的信息进行数字签名；

若否，则不执行对用于生成二维码的信息进行数字签名并向第一服务器发送注册邀请。

21.如权利要求17至20中的任一权利要求所述的装置，其特征在于，处理单元基于非对称加密算法，利用私钥对用于生成二维码的信息进行数字签名。

22.如权利要求21所述的装置，其特征在于，根据生成二维码的信息的不同，在对用于生成二维码的信息进行数字签名的步骤中使用的私钥不同。

23.一种二维码生成系统，其特征在于，所述系统包括第一服务器和第二服务器，第一服务器包括：

发送单元，向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息；

接收单元，从第二服务器接收由第一服务器生成的包含有数字签名的二维码信息；

生成单元，利用所述二维码信息，生成二维码，

第二服务器包括：

接收单元，从第一服务器接收所述请求；

处理单元，对用于生成二维码的信息进行数字签名；

发送单元，将包含有数字签名的二维码信息发送到第一服务器。

24.一种二维码识别方法，其特征在于，包括：

启动与对用于生成二维码的信息进行数字签名的服务器对应的应用；

利用所述应用中的扫描单元扫描所述二维码；

利用公钥对扫描的二维码进行验证；

若验证成功，则识别出与扫描的二维码对应的信息。

25.如权利要求24所述的方法，其特征在于，所述公钥是从所述服务器或远程存储装置获得的。

26.如权利要求24所述的方法，其特征在于，还包括：存储所述验证步骤中相关的信息。

27.一种二维码识别设备，其特征在于，包括：

启动单元，启动与对用于生成二维码的信息进行数字签名的服务器对应的应用；

扫描单元，利用所述应用中的扫描单元扫描所述二维码；

验证单元，利用公钥对扫描的二维码进行验证；

识别单元，在验证单元验证成功的情况下，识别出与扫描的二维码对应的信息。

28.如权利要求27所述的设备，其特征在于，所述公钥是从所述服务器或远程存储装置获得的。

29.如权利要求28所述的设备，其特征在于，还包括：存储单元，存储所述验证步骤中相关的信息。

二维码生成方法及其设备和二维码识别方法及其设备

技术领域

[0001] 本申请涉及图形图像技术领域，特别涉及一种二维码生成方法及其设备和二维码识别方法及其设备。

背景技术

[0002] 二维码又称二维条形码，它通过某种特定几何图形按一定规律在平面(二维方向)上分布形成的条/空相间图形来记录数据符号信息。二维码具有信息容量大、编码范围广、容错力强、译码可靠性高等特点，同时还具有成本低、易制作等优势。因此，二维码在人们生活中得到广泛应用。

[0003] 随着互联网的发展和移动终端的普及，生活中的二维码也随处可见。例如，商家可将支付二维码张贴在付款处，用户可利用应用中的扫描二维码功能进行扫描。或者商家在对商品进行推广时，可将app的下载二维码张贴在人流较多的地方(例如，地铁、商场等)，吸引过往人群扫描二维码进行应用下载。因此，商家或第三方需要向用户提供真实有效的二维码，而用户需要对这些二维码进行有效地校验。

[0004] 在对现有技术的研究和实践过程中，本发明的发明人发现，人们很难从肉眼判断二维码的真伪，并且在二维码识别过程中，手机应用中的扫描单元会在不进行任何验证的情况下直接对各种二维码进行识别。由此可以看出，目前存在如下需求：出于保证二维码真实有效性的考虑而生成二维码的技术方案，相应地也存在这样的需求：在识别二维码时对二维码进行真伪判定的技术方案。

[0005] 上述信息仅作为背景信息被呈现以帮助理解本公开。至于任何上述信息是否可应用为针对本公开的现有技术，尚未做出决定，也未做出声明。

发明内容

[0006] 本发明的主要目的在于提供一种二维码生成方法及其设备和二维码识别方法及其设备，旨在解决上述问题。

[0007] 本发明的一方面提供一种二维码生成方法，包括：第一服务器向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息；第二服务器根据接收到的生成二维码的请求，对用于生成二维码的信息进行数字签名；将包含有数字签名的二维码信息发送到第一服务器；第一服务器利用所述二维码信息，生成二维码。

[0008] 本发明的一方面提供一种二维码生成方法，所述方法由第一服务器执行，包括：向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息；从第二服务器接收由第二服务器生成的包含有数字签名的二维码信息；利用所述二维码信息，生成二维码。

[0009] 本发明的一方面提供二维码生成设备，包括：发送单元，向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息；接收单元，从第二服务器接收由第二服务器生成的包含有数字签名的二维码信息；生成单元，利用所述二维码信息，生成二维码。

[0010] 本发明的一方面提供一种二维码生成方法，所述方法由第二服务器执行，包括：从第一服务器接收生成二维码的请求，所述请求包括用于生成二维码的信息；对用于生成二维码的信息进行数字签名；将包含有数字签名的二维码信息发送到第一服务器。

[0011] 本发明的一方面提供一种二维码生成装置，包括：接收单元，从第一服务器接收生成二维码的请求，所述请求包括用于生成二维码的信息；处理单元，对用于生成二维码的信息进行数字签名；发送单元，将包含有数字签名的二维码信息发送到第一服务器。

[0012] 本发明的一方面提供一种二维码生成系统，所述系统包括第一服务器和第二服务器，第一服务器包括：发送单元，向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息；接收单元，从第二服务器接收由第一服务器生成的包含有数字签名的二维码信息；生成单元，利用所述二维码信息，生成二维码；第二服务器包括：接收单元，从第一服务器接收所述请求；处理单元，对用于生成二维码的信息进行数字签名；发送单元，将包含有数字签名的二维码信息发送到第一服务器。

[0013] 本发明的另一方面提供一种二维码识别方法，包括：启动与对用于生成二维码的信息进行数字签名的服务器对应的应用；利用所述应用中的扫描单元扫描所述二维码；利用公钥对扫描的二维码进行验证；若验证成功，则识别出与扫描的二维码对应的信息。

[0014] 本发明的另一方面提供一种二维码识别设备，包括：启动单元，启动与对用于生成二维码的信息进行数字签名的服务器对应的应用；扫描单元，利用所述应用中的扫描单元扫描所述二维码；验证单元，利用公钥对扫描的二维码进行验证；识别单元，在验证单元验证成功的情况下，识别出与扫描的二维码对应的信息。

[0015] 与现有技术相比，根据本发明的实施例通过一服务器与另一服务器之间协同作用产生二维码，增强了二维码的安全性和有效性，并且方便在二维码识别过程中识别出二维码是否被篡改。此外，根据本发明的另一实施例通过特定应用利用公钥识别出与二维码对应地信息，增加了二维码识别过程中的真伪判定，防止二维码被篡改。

附图说明

[0016] 此处所说明的附图用来提供对本申请的进一步理解，构成本申请的一部分，本申请的示意性实施例及其说明用于解释本申请，并不构成对本申请的不当限定。在附图中：

[0017] 图1是应用根据本发明的实施例的二维码生成方法的场景图；

[0018] 图2是图1中所示出的服务器110与服务器120之间的交互处理的示意图；

[0019] 图3是根据本发明的实施例的识别二维码的示意图；

[0020] 图4是根据本发明的实施例的由第一服务器执行的二维码生成方法的流程图；

[0021] 图5是执行如图4所示的二维码生成方法的二维码生成设备的框图；

[0022] 图6是根据本发明的实施例的由第二服务器执行的二维码生成方法的流程图；

[0023] 图7是执行如图6所示的二维码生成方法的二维码生成设备的框图；

[0024] 图8是根据本发明的实施例的二维码识别方法的流程图；

[0025] 图9是根据本发明的实施例的执行如图8所述的二维码识别方法的二维码识别设备的框图；

[0026] 图10是根据本发明的实施例的电子设备的框图。

具体实施方式

[0027] 为使本申请的目的、技术方案和优点更加清楚，下面将结合本申请具体实施例及相应的附图对本申请技术方案进行清楚、完整地描述。显然，所描述的实施例仅是本申请一部分实施例，而不是全部的实施例。基于本申请中的实施例，本领域普通技术人员在没有做出创造性劳动前提下所获得的所有其他实施例，都属于本申请保护的范围。

[0028] 在下文中，将参照附图更详细地描述实施例。相同的标号始终表示相同的元件。为了更清楚地理解本发明，以下将对本发明所涉及的术语进行解释。

[0029] 终端/电子装置：通常是指网络系统中由用户使用的并用于与服务器进行通信的装置，本发明的实施例提供的二维码生成方法可由二维码生成设备执行，并且本发明的实施例提供的二维码识别方法可由二维码识别设备执行，而二维码生成设备和二维码识别设备可以是终端/电子装置。根据本发明的终端/电子装置可包括但不限于具有显示单元的以下任意设备：个人计算机(PC)、移动装置(诸如，蜂窝电话、个人数字助理(PDA)、数码相机、便携式游戏控制台、MP3播放器、便携式/个人多媒体播放器(PMP)、手持电子书、平板PC、便携式膝上型PC和全球定位系统(GPS)导航仪)、智能TV等。

[0030] 应用(app)：可由用户直接在计算机操作系统(OS)或移动OS上执行的软件，应用可包括存储在终端的存储单元中的嵌入式应用或第三方应用。嵌入式应用是指预先安装在终端中的应用。例如，嵌入式应用可以是浏览器、电子邮件、即时信使等。第三方应用非常多样化，并且是指如下所述从线上市场下载以安装在终端上的应用，例如，支付应用、购物应用、娱乐应用等。

[0031] 图1是应用根据本发明的实施例的二维码生成方法的场景图。

[0032] 如图1所示，服务器110与服务器120以有线或无线方式进行连接，应理解，在本发明的各个实施例中，无线连接可以是一对一的无线连接，例如，蓝牙、近距离无线通信(NFC)等，在安全性有保障的场景中，也可以使用无线局域网(WiFi)。

[0033] 服务器110是用于生成二维码的服务器，例如，服务器110可以是应用服务器、网站服务器等。举例来说，服务器110是支付应用服务器，则应用服务器110可响应于用户输入来生成关于某一商品的二维码。或者服务器110是网站服务器，则可在显示器上显示由服务器110根据需求生成的各种二维码。服务器120是第三方服务器并且是具有权威认证的第三方服务器(例如，支付宝服务器)。

[0034] 应注意，服务器110和服务器120均是提供计算服务的电子装置，可以响应于服务器请求并进行处理，并且这两个服务器的架构与通用计算机的架构类似，在本发明中，服务器110和服务器120提供不同的服务。

[0035] 参照图1，服务器110与服务器120进行交互处理，随后服务器110根据服务器提供的信息生成二维码，这将在以下参照图2进行详细描述，因此省略对其的描述。

[0036] 随后，服务器110可将二维码显示在显示器上，或者直接利用输出设备(例如，打印机等)进行输出。然后，用户可利用移动终端中的扫描单元对二维码进行扫描。

[0037] 以下将参照图2详细说明服务器110与服务器120之间的交互处理。

[0038] 如图2所示，在步骤210，服务器110向服务器120发送生成二维码的请求，所述请求可包括用于生成二维码的信息(以下简称二维码信息)，例如，所述二维码信息可包括收款

人账号信息，或者所述二维码信息可包括网址信息。

[0039] 可选地，服务器110执行步骤210之前预先向服务器120提出注册请求，所述注册请求中可包含与本次注册相关的所有信息，例如，服务器110可向服务器120提供自身的各类资质证明，例如，经营许可证、商品明细等。随后，服务器120在对服务器110提供的信息校验通过后，完成对服务器110的注册。并将服务器110提供的这些资质证明存储在服务器120的存储器中。可选地，可将这些资质证明存储在远程存储器中，这样，在需要调用这些资质证明时，通过远程存储器的地址调用这些资质证明。

[0040] 如此，在服务器110向服务器120发送二维码生成请求之后，服务器120对服务器110进行验证来确定服务器110是否已在服务器120中注册，若否，则服务器120不提供接下来的服务，并提示服务器110进行注册，具体来说，服务器120可拒绝服务器110的二维码生成请求，并向服务器110发出注册邀请。若服务器110已在服务器120中注册，则进行接下来的步骤。

[0041] 通过以上的注册步骤，服务器120可对所有通过验证的装置提供服务，从而能够保证由服务器120协同生成的二维码的合法性。并在与服务器110的商家产生纠纷时留有证据。

[0042] 在步骤220，服务器120可基于非对称加密算法对所述二维码信息进行数字签名。具体来说，服务器120可基于非对称加密算法，利用预先生成的私钥(存储在服务器120中)，对步骤210中的二维码生成请求中的二维码信息进行数字签名。如此一来，在识别二维码的过程中，若利用公钥扫描成功，则表明该二维码为服务器110利用服务器120生成的二维码，若扫描不成功，则表明该二维码很可能是伪造二维码或者仅由服务器110生成未利用服务器120进行处理的二维码。

[0043] 应注意，服务器120根据二维码信息的不同生成不同的数字签名，也就是说，服务器120可根据二维码信息的不同提供不同的私钥，随后利用各个私钥对各个二维码信息进行数字签名。因此，即使是同一网站发送的关于不同商品的不同的链接信息，也使用不同的私钥对不同的链接信息进行数字签名。

[0044] 以上所述的非对称加密算法可称为公钥加密算法，在该算法中，利用公钥对数据进行加密，而利用对应的私钥才能解密，或者利用私钥对数据进行加密，而利用对应的公钥进行解密。根据示例性实施例，非对称加密算法可包括RSA公钥加密算法、Elgamal加密算法、背包算法、椭圆曲线加密算法(ECC)加密算法。由于本发明的发明目的在于保证二维码真实有效性，优选地，可选择RSA公钥加密算法对生成的交易数据进行加密。

[0045] 由于利用非对称加密算法对数据进行数字签名是本领域常见的技术手段，在此将省略对其的详细描述。应注意，虽然以上示出了非对称加密算法的示例，但本领域技术人员应理解，所有能够生成数字签名的非对称加密算法都可应用于此。

[0046] 随后，在步骤130，服务器120将包含数字签名的二维码信息发送到服务器110。服务器110在接收到包含数字签名的二维码信息之后，在步骤140，利用包含数字签名的二维码信息生成二维码。具体来说，可基于二维码生成算法，利用二维码信息和数字签名生成二维码。优选的，二维码生成算法包括快速反应码(Quickresponse code,QRcode)算法。

[0047] 由于利用二维码生成算法生成二维码是本领域常见的技术手段，在此将省略对其的详细描述。本领域技术人员应理解，所有能够生成二维码的二维码生成算法都可应用于

此。

[0048] 接下来将参照图3详细描述对二维码进行验证的示意图。

[0049] 如图3所示，用户可利用移动终端对显示器上显示的电子二维码或经由输出设备输出的二维码进行验证。

[0050] 用户启动与服务器120对应的应用，例如，用户可在移动终端中启动与支付宝服务器对应的支付宝应用。随后，用户利用所述应用中的扫描单元对显示在显示器上的二维码或打印出来的二维码进行扫描。

[0051] 应注意，用户在进行二维码识别过程中，必须利用与服务器120对应的应用中的扫描单元。这是由于在与服务器120对应的应用包含或可获取与二维码对应的公钥。

[0052] 可选地，在利用所述应用中的扫描单元对二维码进行扫描之后，可向服务器120或存储有公钥的远程存储器获取公钥。随后，利用所述公钥对扫描的二维码进行验证，若验证成功，则可成功识别出二维码以进行下一步操作。也就是说，可根据二维码识别结果，在移动终端的显示界面上显示与所述二维码对应的操作界面，例如，如果二维码的识别结果是关于支付宝的链接，则移动终端调用支付宝应用，从而在显示单元上显示关于支付宝的操作界面，如果二维码的识别结果是关于微信的链接，则移动终端调用微信应用，从而在显示单元上显示关于微信的操作界面。如果二维码的识别结果是关于网址的链接，则移动终端调用浏览器应用，从而在显示单元上显示关于浏览器的操作界面。

[0053] 若验证不成功，则说明二维码被篡改。此外，还存在这种情况：篡改二维码的操作者同样在服务器120上注册，并且用于篡改原始二维码的二维码同样是在服务器120的协同下生成。例如，商家乙将商家甲张贴在外的二维码撕掉，张贴他自己的二维码。在这种情况下，利用与服务器120对应的应用中的扫描单元能够成功识别商家乙的二维码。为了解决这种情况，可记录以上所述的扫描过程。这样可根据扫描记录确定篡改二维码的操作者，并根据操作者在注册阶段提供的信息来确定操作者的身份。

[0054] 图4是根据本发明的实施例的由第一服务器执行的二维码生成方法的流程图。

[0055] 在步骤S410，向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息。

[0056] 在步骤S420，从第二服务器接收由第二服务器生成的包含有数字签名的二维码信息。

[0057] 在步骤S430，利用所述二维码信息，生成二维码。

[0058] 在可替换实施例中，向第二服务器发送生成二维码的请求之前还包括：向第二服务器发送注册请求，所述注册请求包括与本次注册相关的所有信息。

[0059] 图5是执行如图4所示的二维码生成方法的二维码生成设备(即，第一服务器)的框图。

[0060] 本领域技术人员将理解，图5中示出的二维码生成设备的结构并不构成对本发明的电子装置的限定，可包括比图示更多或更少的部件，或组合某些部件，或不同的部件布置。

[0061] 如图5所示，二维码生成设备可包括发送单元510、接收单元520和生成单元530。

[0062] 发送单元510可向第二服务器发送生成二维码的请求，所述请求包括用于生成二维码的信息。

[0063] 接收单元520可从第二服务器接收由第二服务器生成的包含有数字签名的二维码信息；

[0064] 生成单元530可利用所述二维码信息，生成二维码。

[0065] 在可替换实施例中，发送单元510在向第一服务器发送生成二维码的请求之前，向第一服务器发送注册请求，所述注册请求包括与本次注册相关的所有信息。

[0066] 图6是根据本发明的实施例的由第二服务器执行的二维码生成方法的流程图。

[0067] 在步骤S610，从第一服务器接收生成二维码的请求，所述请求包括用于生成二维码的信息；

[0068] 在步骤S620，对用于生成二维码的信息进行数字签名；

[0069] 在步骤S630，将包含有数字签名的二维码信息发送到第一服务器。

[0070] 在可选实施例中，在从第一服务器接收生成二维码的请求之前还包括：从第一服务器接收注册请求，所述注册请求包括与本次注册相关的所有信息。并且，在从第一服务器接收到注册请求之后，所述二维码生成方法还可包括：根据所述注册请求，完成对第一服务器的注册。

[0071] 图7是执行如图6所示的二维码生成方法的二维码生成设备(即，第二服务器)的框图。

[0072] 本领域技术人员将理解，图7中示出的二维码生成设备的结构并不构成对本发明的电子装置的限定，可包括比图示更多或更少的部件，或组合某些部件，或不同的部件布置。

[0073] 所述二维码生成设备可包括接收单元710、处理单元720和发送单元730。

[0074] 接收单元710从第一服务器接收生成二维码的请求，所述请求包括用于生成二维码的信息。在可替换实施例中，接收单元还从第一服务器接收注册请求，所述注册请求包括与本次注册相关的所有信息。

[0075] 在可替换实施例中，所述二维码生成设备可包括注册单元，所述注册单元根据所述注册请求，完成对第一服务器的注册。

[0076] 处理单元720对用于生成二维码的信息进行数字签名。可选地，处理单元720可基于非对称加密算法，利用私钥对用于生成二维码的信息进行数字签名。

[0077] 发送单元730将包含有数字签名的二维码信息发送到第一服务器。

[0078] 在可替换实施例中，所述二维码生成设备还包括确定单元，所述确定单元确定第一服务器是否在第二服务器中注册：若是，则根据接收到的生成二维码的请求对用于生成二维码的信息进行数字签名；若否，则不执行对用于生成二维码的信息进行数字签名并向第一服务器发送注册邀请。

[0079] 在可替换的实施例中，根据生成二维码的信息的不同，在对用于生成二维码的信息进行数字签名的步骤中使用的私钥不同。

[0080] 在另一示例性实施例中，可提供一种二维码生成系统，所述系统包括如图5中的二维码生成设备和如图7所述的二维码生成设备。

[0081] 如上所述，根据本发明的实施例提供的二维码生成方法及其设备通过一服务器与另一服务器之间协同作用产生二维码，增强了二维码的安全性和有效性，并且方便在二维码识别过程中识别出二维码是否被篡改。

[0082] 图8是根据本发明的实施例的二维码识别方法的流程图。

[0083] 在步骤S810，启动与对用于生成二维码的信息进行数字签名的服务器对应的应用。

[0084] 在步骤S820，利用所述应用中的扫描单元扫描所述二维码。

[0085] 在步骤S830，利用公钥对扫描的二维码进行验证。

[0086] 在步骤S840，若验证成功，则识别出与扫描的二维码对应的信息。

[0087] 在可替换实施例中，所述公钥是从所述服务器或远程存储装置获得的。此外，所述方法还可包括存储所述验证步骤中相关的信息。

[0088] 图9是根据本发明的实施例的执行如图8所述的二维码识别方法的二维码识别设备的框图。

[0089] 本领域技术人员将理解，图9中示出的二维码识别设备的结构并不构成对本发明的电子装置的限定，可包括比图示更多或更少的部件，或组合某些部件，或不同的部件布置。

[0090] 所述二维码识别设备可包括启动单元910、扫描单元920、验证单元930和识别单元940。

[0091] 启动单元910可启动与对用于生成二维码的信息进行数字签名的服务器对应的应用。

[0092] 扫描单元920可利用所述应用中的扫描单元扫描所述二维码；

[0093] 验证单元930可利用公钥对扫描的二维码进行验证；

[0094] 识别单元940可在验证单元验证成功的情况下，识别出与扫描的二维码对应的信息。

[0095] 在可替换实施例中，所述公钥是从所述服务器或远程存储装置获得的。

[0096] 在可替换实施例中，所述二维码识别设备还包括存储单元，所述存储单元存储所述验证步骤中相关的信息。

[0097] 图10是执行根据本发明的实施例的二维码生成方法或二维码识别方法的电子设备的框图。参考图10，在硬件层面，该电子设备包括处理器、内部总线、网络接口、内存以及非易失性存储器，当然还可能包括其他业务所需要的硬件。处理器从非易失性存储器中读取对应的计算机程序到内存中然后运行，在逻辑层面上形成的网页截图装置。当然，除了软件实现方式之外，本申请并不排除其他实现方式，比如逻辑器件抑或软硬件结合的方式等等，也就是说以下处理流程的执行主体并不限定于各个逻辑单元，也可以是硬件或逻辑器件。

[0098] 根据本发明的实施例提供的二维码识别方法及其设备通过特定应用利用公钥识别出与二维码对应地信息，增加了二维码识别过程中的真伪判定，防止二维码被篡改。

[0099] 在20世纪90年代，对于一个技术的改进可以很明显地区分是硬件上的改进(例如，对二极管、晶体管、开关等电路结构的改进)还是软件上的改进(对于方法流程的改进)。然而，随着技术的发展，当今的很多方法流程的改进已经可以视为硬件电路结构的直接改进。设计人员几乎都通过将改进的方法流程编程到硬件电路中来得到相应的硬件电路结构。因此，不能说一个方法流程的改进就不能用硬件实体模块来实现。例如，可编程逻辑器件(Programmable Logic Device,PLD)(例如现场可编程门阵列(Field Programmable Gate

Array,FPGA))就是这样一种集成电路,其逻辑功能由用户对器件编程来确定。由设计人员自行编程来把一个数字系统“集成”在一片PLD上,而不需要请芯片制造厂商来设计和制作专用的集成电路芯片。而且,如今,取代手工地制作集成电路芯片,这种编程也多半改用“逻辑编译器(logic compiler)”软件来实现,它与程序开发撰写时所用的软件编译器相类似,而要编译之前的原始代码也得用特定的编程语言来撰写,此称之为硬件描述语言(Hardware Description Language,HDL),而HDL也并非仅有一种,而是有许多种,如ABEL(Advanced Boolean Expression Language)、AHDL(Altera Hardware Description Language)、Confluence、CUPL(Cornell University Programming Language)、HDCal、JHDL(Java Hardware Description Language)、Lava、Lola、MyHDL、PALASM、RHDL(Ruby Hardware Description Language)等,目前最普遍使用的是VHDL(Very-High-Speed Integrated Circuit Hardware Description Language)与Verilog。本领域技术人员也应该清楚,只需要将方法流程用上述几种硬件描述语言稍作逻辑编程并编程到集成电路中,就可以很容易得到实现该逻辑方法流程的硬件电路。

[0100] 控制器可以按任何适当的方式实现,例如,控制器可以采取例如微处理器或处理器以及存储可由该(微)处理器执行的计算机可读程序代码(例如软件或固件)的计算机可读介质、逻辑门、开关、专用集成电路(Application Specific Integrated Circuit,ASIC)、可编程逻辑控制器和嵌入微控制器的形式,控制器的例子包括但不限于以下微控制器:ARC 625D、Atmel AT91SAM、Microchip PIC18F26K20以及Silicone Labs C8051F320,存储器控制器还可以被实现为存储器的控制逻辑的一部分。本领域技术人员也知道,除了以纯计算机可读程序代码方式实现控制器以外,完全可以通过将方法步骤进行逻辑编程来使得控制器以逻辑门、开关、专用集成电路、可编程逻辑控制器和嵌入微控制器等的形式来实现相同功能。因此这种控制器可以被认为是一种硬件部件,而对其内包括的用于实现各种功能的装置也可以视为硬件部件内的结构。或者甚至,可以将用于实现各种功能的装置视为既可以是实现方法的软件模块又可以是硬件部件内的结构。

[0101] 上述实施例阐明的系统、装置、模块或单元,具体可以由计算机芯片或实体实现,或者由具有某种功能的产品来实现。一种典型的实现设备为计算机。具体的,计算机例如可以为个人计算机、膝上型计算机、蜂窝电话、相机电话、智能电话、个人数字助理、媒体播放器、导航设备、电子邮件设备、游戏控制台、平板计算机、可穿戴设备或者这些设备中的任何设备的组合。

[0102] 为了描述的方便,描述以上装置时以功能分为各种单元分别描述。当然,在实施本申请时可以把各单元的功能在同一个或多个软件和/或硬件中实现。

[0103] 本领域内的技术人员应明白,本申请的实施例可提供为方法、系统、或计算机程序产品。因此,本申请可采用完全硬件实施例、完全软件实施例、或结合软件和硬件方面的实施例的形式。而且,本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0104] 本申请是参照根据本申请实施例的方法、设备(系统)、和计算机程序产品的流程图和/或方框图来描述的。应理解可由计算机程序指令实现流程图和/或方框图中的每一流程和/或方框、以及流程图和/或方框图中的流程和/或方框的结合。可提供这些计算机程序

指令到通用计算机、专用计算机、嵌入式处理机或其他可编程数据处理设备的处理器以产生一个机器，使得通过计算机或其他可编程数据处理设备的处理器执行的指令产生用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的装置。

[0105] 这些计算机程序指令也可存储在能引导计算机或其他可编程数据处理设备以特定方式工作的计算机可读存储器中，使得存储在该计算机可读存储器中的指令产生包括指令装置的制造品，该指令装置实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能。

[0106] 这些计算机程序指令也可装载到计算机或其他可编程数据处理设备上，使得在计算机或其他可编程设备上执行一系列操作步骤以产生计算机实现的处理，从而在计算机或其他可编程设备上执行的指令提供用于实现在流程图一个流程或多个流程和/或方框图一个方框或多个方框中指定的功能的步骤。

[0107] 在一个典型的配置中，计算设备包括一个或多个处理器(CPU)、输入/输出接口、网络接口和内存。

[0108] 内存可能包括计算机可读介质中的非永久性存储器，随机存取存储器(RAM)和/或非易失性内存等形式，如只读存储器(ROM)或闪存(flash RAM)。内存是计算机可读介质的示例。

[0109] 计算机可读介质包括永久性和非永久性、可移动和非可移动媒体可以由任何方法或技术来实现信息存储。信息可以是计算机可读指令、数据结构、程序的模块或其他数据。计算机的存储介质的例子包括，但不限于相变内存(PRAM)、静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)、其他类型的随机存取存储器(RAM)、只读存储器(ROM)、电可擦除可编程只读存储器(EEPROM)、快闪记忆体或其他内存技术、只读光盘只读存储器(CD-ROM)、数字多功能光盘(DVD)或其他光学存储、磁盒式磁带，磁带磁磁盘存储或其他磁性存储设备或任何其他非传输介质，可用于存储可以被计算设备访问的信息。按照本文中的界定，计算机可读介质不包括暂存电脑可读媒体(transitory media)，如调制的数据信号和载波。

[0110] 还需要说明的是，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、商品或者设备不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、商品或者设备所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括所述要素的过程、方法、商品或者设备中还存在另外的相同要素。

[0111] 本领域技术人员应明白，本申请的实施例可提供为方法、系统或计算机程序产品。因此，本申请可采用完全硬件实施例、完全软件实施例或结合软件和硬件方面的实施例的形式。而且，本申请可采用在一个或多个其中包含有计算机可用程序代码的计算机可用存储介质(包括但不限于磁盘存储器、CD-ROM、光学存储器等)上实施的计算机程序产品的形式。

[0112] 本申请可以在由计算机执行的计算机可执行指令的一般上下文中描述，例如程序模块。一般地，程序模块包括执行特定任务或实现特定抽象数据类型的例程、程序、对象、组件、数据结构等等。也可以在分布式计算环境中实践本申请，在这些分布式计算环境中，由通过通信网络而被连接的远程处理设备来执行任务。在分布式计算环境中，程序模块可以位于包括存储设备在内的本地和远程计算机存储介质中。

[0113] 本说明书中的各个实施例均采用递进的方式描述，各个实施例之间相同相似的部分互相参见即可，每个实施例重点说明的都是与其他实施例的不同之处。尤其，对于系统实施例而言，由于其基本相似于方法实施例，所以描述的比较简单，相关之处参见方法实施例的部分说明即可。

[0114] 以上所述仅为本申请的实施例而已，并不用于限制本申请。对于本领域技术人员来说，本申请可以有各种更改和变化。凡在本申请的精神和原理之内所作的任何修改、等同替换、改进等，均应包含在本申请的权利要求范围之内。

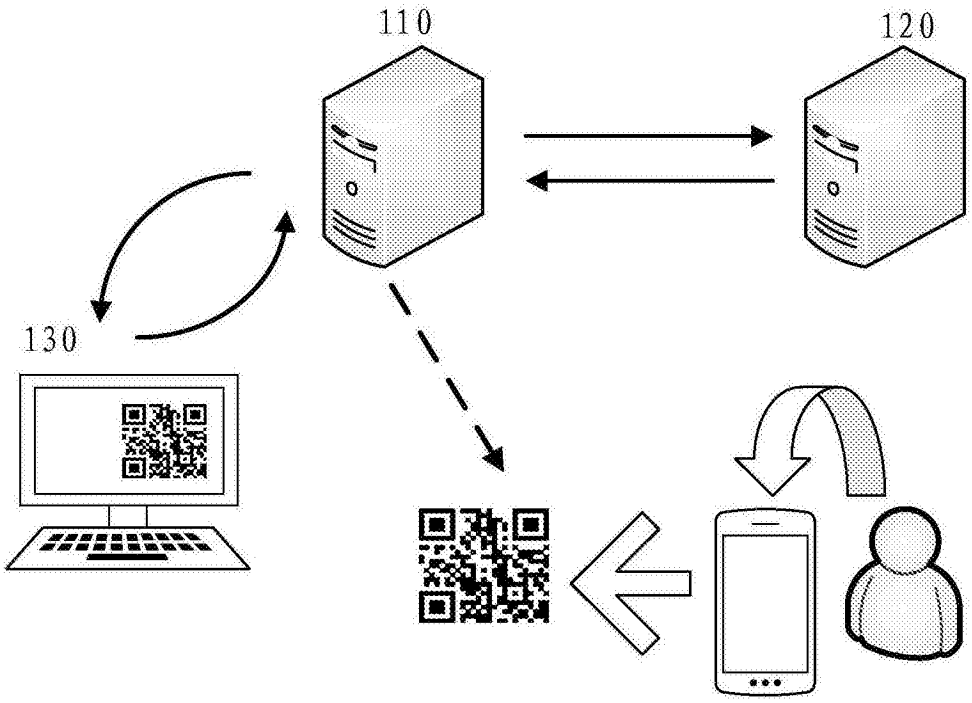

110
120
130

图1

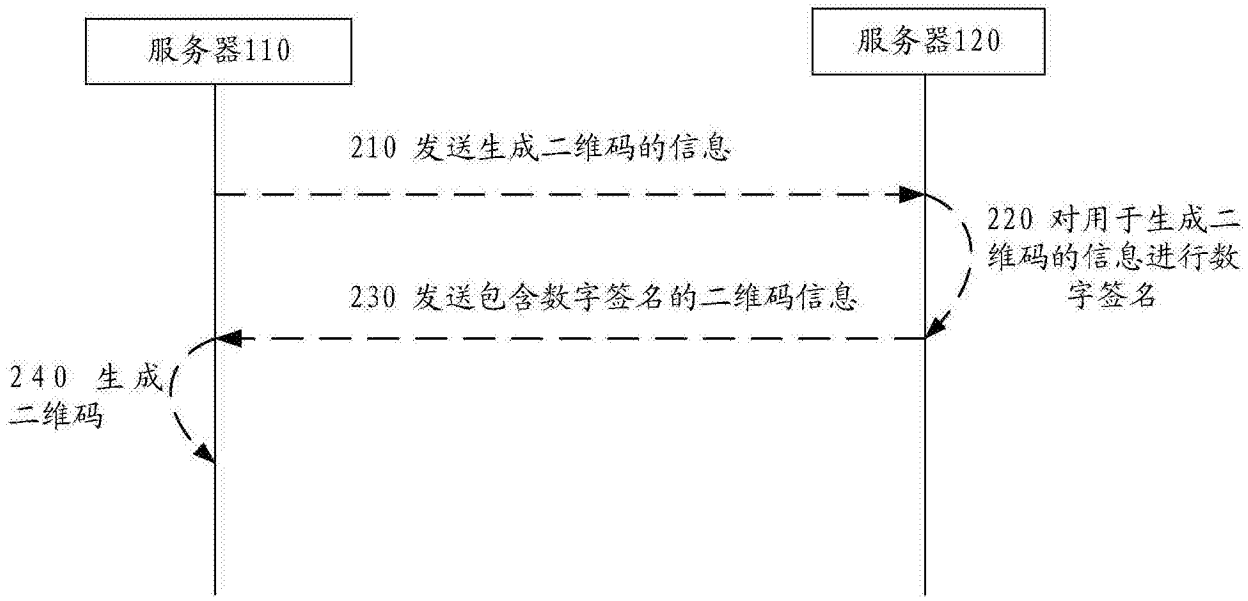

服务器110
服务器120
210 发送生成二维码的信息
220 对用于生成二维码的信息进行数字签名
230 发送包含数字签名的二维码信息
240 生成二维码

图2

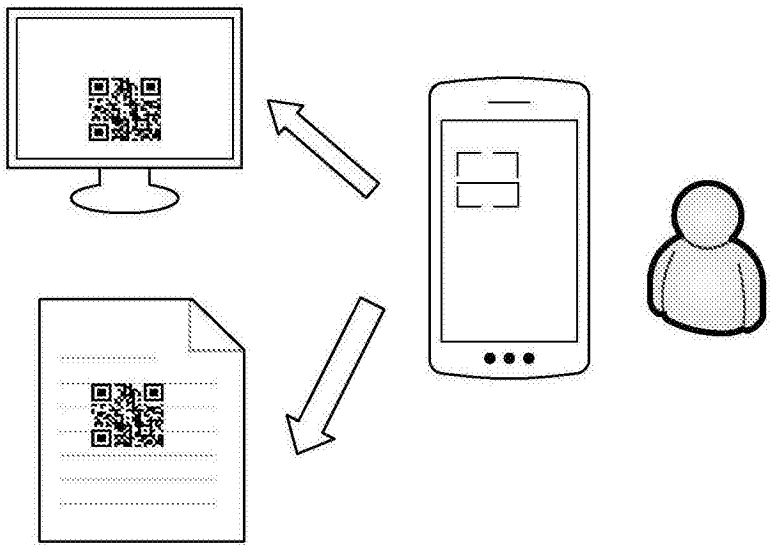


图3

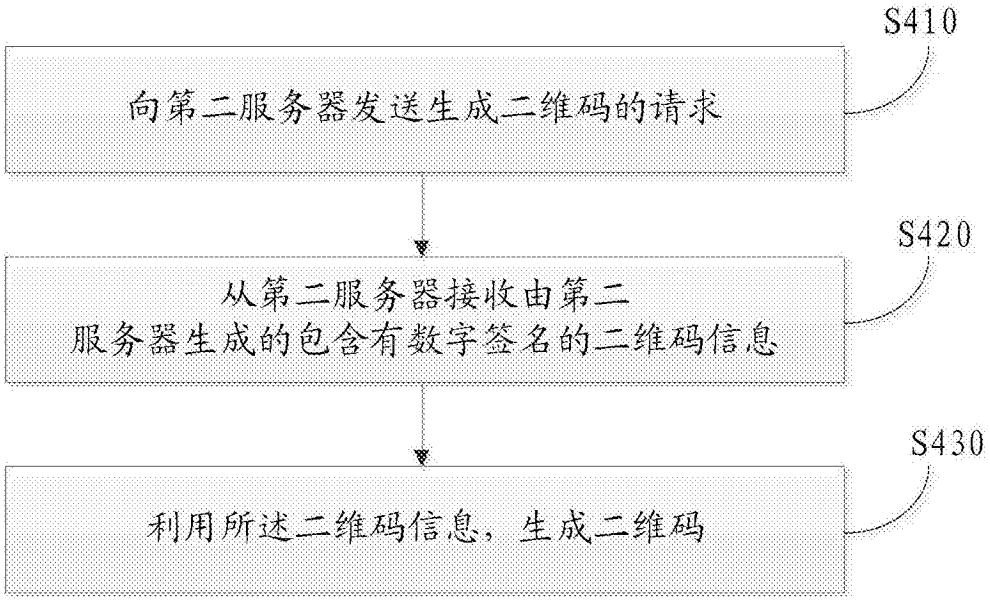

S410
向第二服务器发送生成二维码的请求
S420
从第二服务器接收由第二
服务器生成的包含有数字签名的二维码信息
S430
利用所述二维码信息，生成二维码

图4

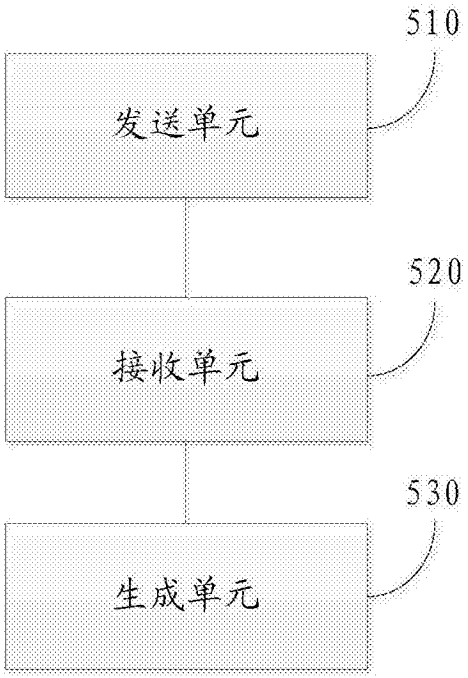

510
发送单元
520
接收单元
530
生成单元

图5

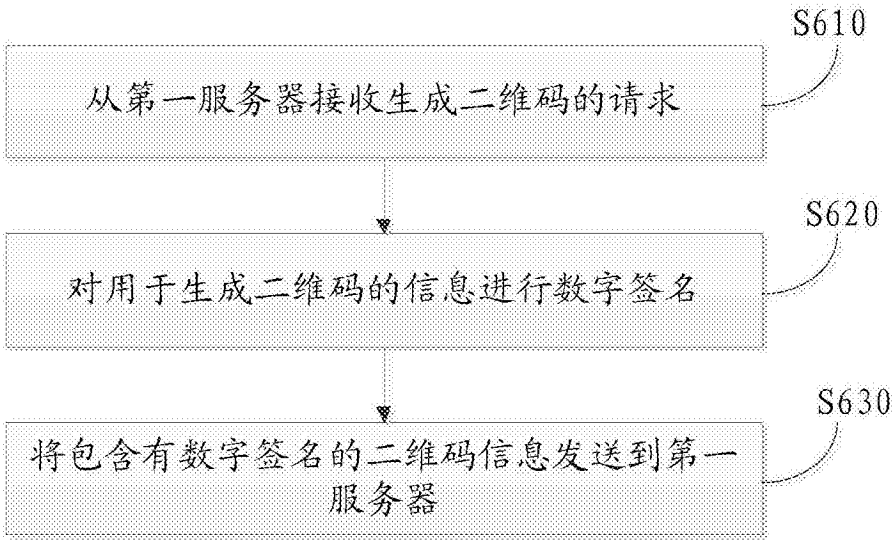

S610
从第一服务器接收生成二维码的请求
S620
对用于生成二维码的信息进行数字签名
S630
将包含有数字签名的二维码信息发送到第一服务器

图6

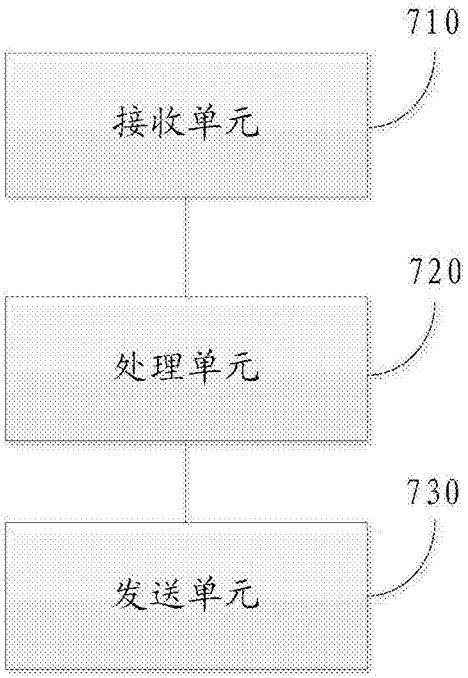

710
接收单元
720
处理单元
730
发送单元

图7

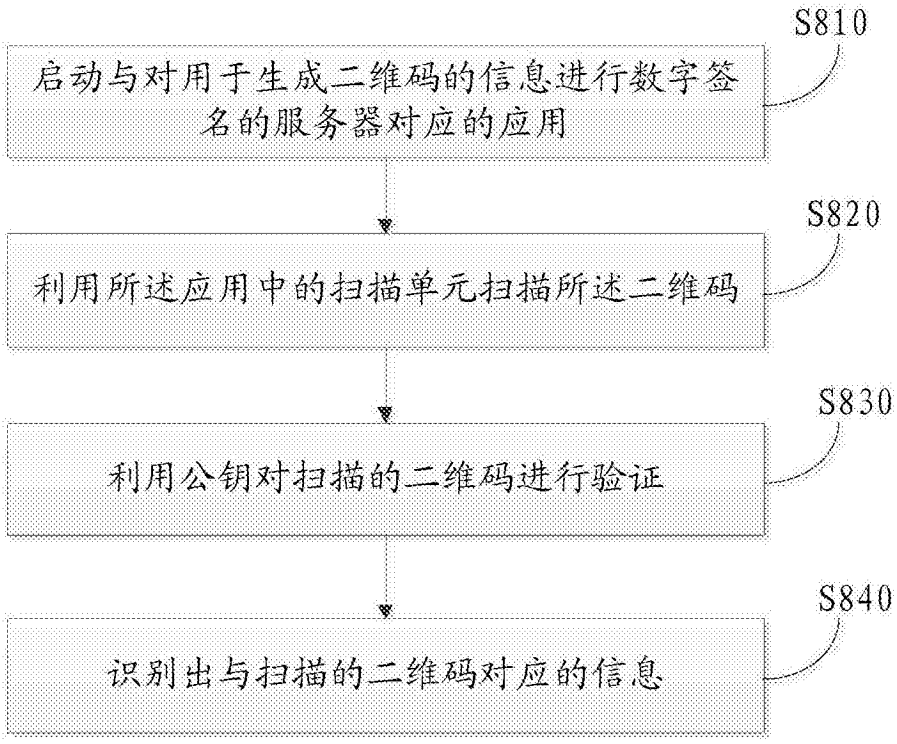

S810
启动与对用于生成二维码的信息进行数字签名的服务器对应的应用
S820
利用所述应用中的扫描单元扫描所述二维码
S830
利用公钥对扫描的二维码进行验证
S840
识别出与扫描的二维码对应的信息

图8

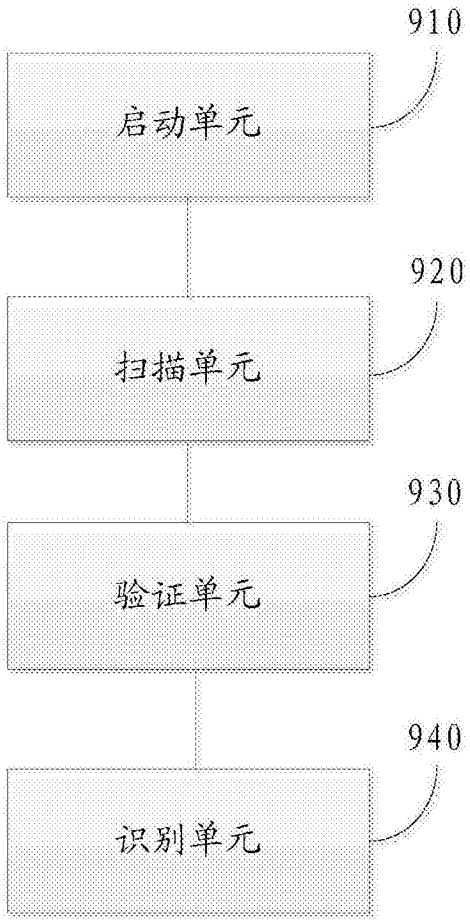


图9

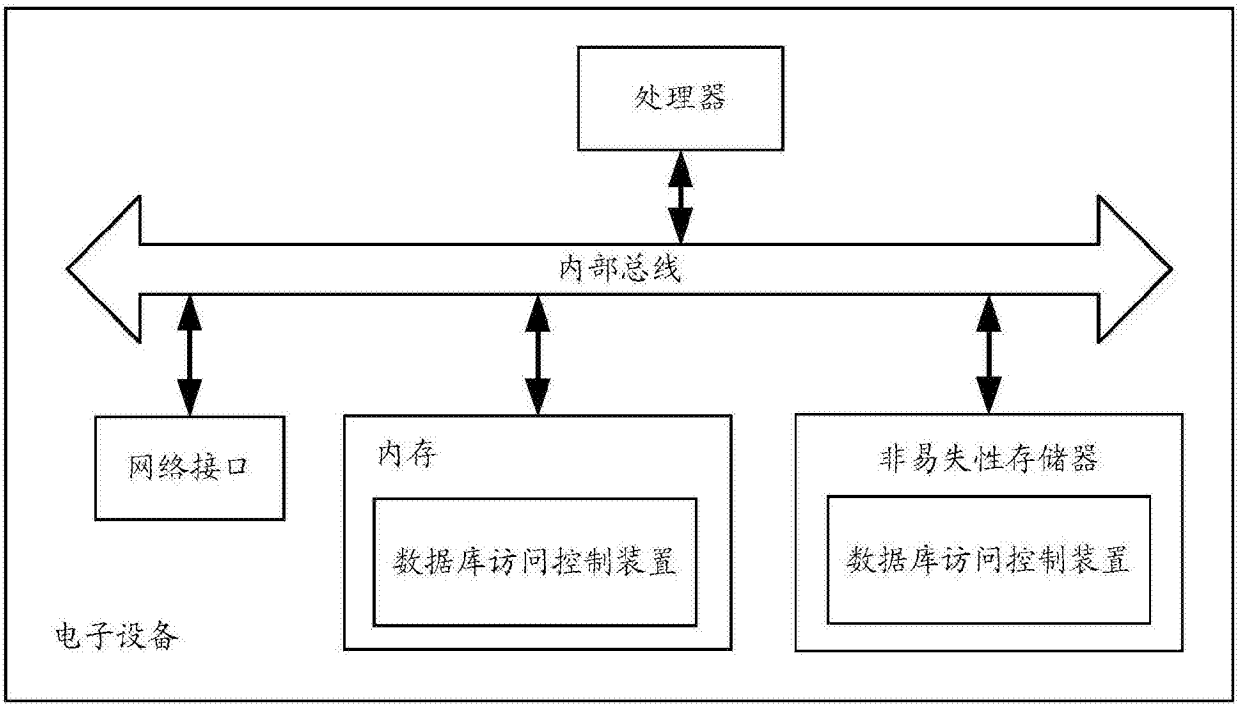


图10