

二维码的提供、验证方法和装置

技术领域

[01] 本说明书实施例涉及二维码技术领域，更具体地，涉及二维码的提供、验证方法和装置。

5 背景技术

[02] 二维码又称二维条码，常见的二维码为 QR 码（Quick Response Code），是一个近几年来移动设备上非常流行的一种编码方式，其相比于传统的条形码可以存储更多的信息，也可以表示更多的数据类型。

- [03] 随着线下支付的不断推广，利用二维码作为收款码、引流入口等目前已广泛流行。
- 10 例如，商户可以把二维码收款码打印出来，张贴在收银台上，以便于用户进行扫码支付。又例如，平台在对其进行推广时，可将其 app 的下载二维码张贴在人流较多的地方，吸引过往人群通过扫描二维码进行 app 的下载。

- [04] 现在存在这样的风险，商户张贴的二维码有可能被他人用自己的二维码替换。而在商户的二维码被替换时，由于二维码本身很难识别，使得商户很难发现自己的二维码被
- 15 替换了。虽然二维码中包括具备差异性的标识（logo）区域，但由于他人可将自己的二维码中 logo 区域自定义为商户的 logo，从而仍然使得商户难以发现二维码是否被替换。而在商户二维码被替换的情况中，当用户支付时，交易涉及的款项，则进入到他人账户而非商户账户，进而给用户或商户带来资金损失。

[05] 因此，需要一种更有效的二维码的提供、验证方案。

20 发明内容

[06] 本说明书实施例旨在提供一种更有效的二维码的提供、验证方案，以解决现有技术中的不足。

[07] 为实现上述目的，本说明书一个方面提供一种提供二维码的方法，包括：

- [08] 从第一用户的终端接收二维码生成请求，所述请求中包括该二维码对应的业务数据，
- 25 其中，所述业务数据包括所述第一用户的用户标识；

[09] 获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

- [10] 存储所述用户标识与所述第一图片的关联关系;
- [11] 基于所述业务数据生成二维码; 以及
- [12] 将所述二维码和所述第一图片提供给所述第一用户。
- [13] 本说明书另一方面提供一种提供二维码的方法, 包括:
- 5 [14] 从第一用户的终端接收二维码生成请求, 所述请求中包括该二维码对应的业务数据, 其中, 所述业务数据包括所述第一用户的用户标识;
- [15] 获取第一图片以与所述用户标识相对应, 其中, 所述第一图片为肉眼可识别图片;
- [16] 存储所述用户标识与所述第一图片的关联关系;
- [17] 基于所述第一图片与所述业务数据生成二维码; 以及
- 10 [18] 将所述二维码和所述第一图片提供给所述第一用户。
- [19] 在一个实施例中, 将所述二维码和所述第一图片提供给所述第一用户包括, 通过叠加所述第一图片和所述二维码获取业务码, 以及, 将所述业务码提供给所述第一用户。
- [20] 在一个实施例中, 所述第一图片为二维码识别设备能够读取的图片。
- [21] 在一个实施例中, 所述第一图片位于所述二维码内部。
- 15 [22] 在一个实施例中, 所述第一图片的面积基于所述二维码的纠错级别确定。
- [23] 在一个实施例中, 所述第一图片包括以下至少一种内容: 图案、文字、数字、符号。
- [24] 在一个实施例中, 所述第一图片的用于对应于其他用户标识的重复获取率低于第一预定值。
- [25] 在一个实施例中, 所述用户标识与所述第一图片唯一对应。
- 20 [26] 在一个实施例中, 获取与所述用户标识对应的第一图片包括, 从预先建立的图库中获取与所述用户标识对应的第一图片, 其中, 所述图库包括数量多于预定值的图片。
- [27] 在一个实施例中, 所述方法还包括, 在从预先建立的图库中获取与所述用户标识对应的第一图片之后, 在所述图库中对所述第一图片进行标记。
- [28] 在一个实施例中, 从预先建立的图库中获取与所述用户标识对应的第一图片包括,
- 25 从预先建立的图库中随机获取与所述用户标识对应的第一图片。
- [29] 在一个实施例中, 所述第一图片的图像数据量小于等于第二预定值。

- [30]在一个实施例中,基于所述第一图片与所述业务数据生成二维码包括,通过预定加密方法对所述第一图片与所述业务数据的组合进行加密以获取加密数据,并基于所述加密数据生成二维码。
- [31]本说明书另一方面提供一种验证二维码的方法,包括:
- 5 [32]从第二用户的终端接收二维码信息和第一图片;
- [33]基于所述二维码信息,获取二维码的内容数据;
- [34]基于所述二维码的内容数据,获取业务数据,其中,所述业务数据中包括第三用户的用户标识;
- [35]基于预存的用户标识与图片的关联关系,获取与所述第三用户的用户标识对应的第
- 10 三图片;
- [36]确定所述第一图片与所述第三图片是否一致;以及
- [37]在所述第一图片与所述第三图片不一致的情况下,确定所述验证不通过。
- [38]本说明书另一方面提供一种验证二维码的方法,包括:
- [39]从第二用户的终端接收二维码信息和第一图片;
- 15 [40]基于所述二维码信息,获取二维码的内容数据;
- [41]基于所述二维码的内容数据,获取业务数据和第二图片信息;
- [42]基于所述第一图片和所述第二图片信息,确定所述第一图片与所述第二图片的相似度;以及
- [43]在所述相似度低于预定阈值时,确定所述验证不通过。
- 20 [44]在一个实施例中,基于所述二维码的内容数据,获取业务数据和第二图片信息包括,通过预定解密方法对所述二维码的内容数据进行解密,从而获取业务数据和第二图片。
- [45]在一个实施例中,从第二用户的终端接收二维码信息和第一图片包括,从第二用户的终端接收业务码,其中,所述业务码中包括叠加的二维码和所述第一图片。
- [46]在一个实施例中,所述二维码信息包括二维码的内容数据。
- 25 [47]在一个实施例中,所述业务数据包括第三用户的用户标识,所述方法还包括:
- [48]在所述第一图片与所述第二图片相似度高于预定阈值的情况下,基于预存的用户标

识与图片的关联关系，获取与所述第三用户的用户标识对应的第三图片；

[49]确定所述第一图片与所述第三图片是否一致；以及

[50]在所述第一图片与所述第三图片不一致的情况中，确定所述验证不通过。

[51]在一个实施例中，所述方法还包括：

5 [52]在所述第一图片与所述第三图片一致的情况中，确定所述验证通过；以及

[53]将所述业务数据发送给所述第二用户的终端。

[54]本说明书另一方面提供一种提供二维码的装置，包括：

[55]接收单元，配置为，从第一用户的终端接收二维码生成请求，所述请求中包括该二维码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；

10 [56]获取单元，配置为，获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

[57]存储单元，配置为，存储所述用户标识与所述第一图片的关联关系；

[58]生成单元，配置为，基于所述业务数据生成二维码；以及

[59]提供单元，配置为，将所述二维码和所述第一图片提供给所述第一用户。

15 [60]本说明书另一方面提供一种提供二维码的装置，包括：

[61]接收单元，配置为，从第一用户的终端接收二维码生成请求，所述请求中包括该二维码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；

[62]获取单元，配置为，获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

20 [63]存储单元，配置为，存储所述用户标识与所述第一图片的关联关系；

[64]生成单元，配置为，基于所述第一图片与所述业务数据生成二维码；以及

[65]提供单元，配置为，将所述二维码和所述第一图片提供给所述第一用户。

[66]在一个实施例中，所述提供单元还包括，叠加子单元，配置为，通过叠加所述第一图片和所述二维码获取业务码，以及，提供子单元，配置为，将所述业务码提供给所述
25 第一用户的终端。

[67]在一个实施例中，所述获取单元还配置为，从预先建立的图库中获取与所述用户标

识对应的第一图片，其中，所述图库包括数量多于预定值的图片。

[68]在一个实施例中，所述装置还包括标记单元，配置为，在从预先建立的图库中获取与所述用户标识对应的第一图片之后，在所述图库中对所述第一图片进行标记。

[69]在一个实施例中，所述获取单元还配置为，从预先建立的图库中随机获取与所述用户标识对应的第一图片。

[70]在一个实施例中，所述生成单元包括，加密子单元，配置为，通过预定加密方法对所述第一图片与所述业务数据的组合进行加密以获取加密数据，以及生成子单元，配置为，基于所述加密数据生成二维码。

[71]本说明书另一方面提供一种验证二维码的装置，包括：

10 [72]接收单元，配置为，从第二用户的终端接收二维码信息和第一图片；

[73]第一获取单元，配置为，基于所述二维码信息，获取二维码的内容数据；

[74]第二获取单元，配置为，基于所述二维码的内容数据，获取业务数据，其中，所述业务数据中包括第三用户的用户标识；

[75]第三获取单元，配置为，基于预存的用户标识与图片的关联关系，获取与所述第三用户的用户标识对应的第三图片；

[76]第一确定单元，配置为，确定所述第一图片与所述第三图片是否一致；以及

[77]第二确定单元，配置为，在所述第一图片与所述第三图片不一致的情况中，确定所述验证不通过。

[78]在一个实施例中，所述装置还包括：

20 [79]第三确定单元，配置为，在所述第一图片与所述第三图片一致的情况中，确定所述验证通过；以及

[80]发送单元，配置为，将所述业务数据发送给所述第二用户的终端。

[81]本说明书另一方面提供一种验证二维码的装置，包括：

[82]接收单元，配置为，从第二用户的终端接收二维码信息和第一图片；

25 [83]第一获取单元，配置为，基于所述二维码信息，获取二维码的内容数据；

[84]第二获取单元，配置为，基于所述二维码的内容数据，获取业务数据和第二图片信息；

- [85]第一确定单元，配置为，基于所述第一图片和所述第二图片信息，确定所述第一图片与所述第二图片的相似度；以及
- [86]第二确定单元，配置为，在所述相似度低于预定阈值时，确定所述验证不通过。
- [87]在一个实施例中，所述第二获取单元还配置为，通过预定解密方法对所述二维码的内容数据进行解密，从而获取业务数据和第二图片。
- 5 [88]在一个实施例中，所述接收单元还配置为，从第二用户的终端接收业务码，其中，所述业务码中包括叠加的二维码和所述第一图片。
- [89]在一个实施例中，所述业务数据包括第三用户的用户标识，所述装置还包括：
- [90]第三获取单元，配置为，在所述第一图片与所述第二图片相似度高于预定阈值的情况中，基于预存的用户标识与图片的关联关系，获取与所述第三用户的用户标识对应的第三图片；
- 10 [91]第三确定单元，配置为，确定所述第一图片与所述第三图片是否一致；以及
- [92]第四确定单元，配置为，在所述第一图片与所述第三图片不一致的情况中，确定所述验证不通过。
- 15 [93]在一个实施例中，所述装置还包括：
- [94]第五确定单元，配置为，在所述第一图片与所述第三图片一致的情况中，确定所述验证通过；以及
- [95]发送单元，配置为，将所述业务数据发送给所述第二用户的终端。
- [96]本说明书另一方面提供一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述任一种方法。
- 20 [97]根据本说明书实施例的二维码方案与传统的二维码相比，增加“验证图片”，验证图片所携带和展示的信息与二维码主体呈基本唯一对应的关系，并且验证图片具有明显区分度，从而使得：当二维码整体被替换(主体+验证图片)时，用户（例如商户或消费者）很容易肉眼发现。当二维码主体被替换，而验证图片保留时，整体的流程会被服务器端
- 25 判断为校验不通过，流程中断，从而避免资金损失或其他风险。

附图说明

- [98]通过结合附图描述本说明书实施例，可以使得本说明书实施例更加清楚：

- [99] 图 1 示出根据本说明书实施例的基于二维码的业务系统 100 的示意图;
- [100] 图 2 示出根据本说明书实施例的一种提供二维码的方法流程图;
- [101] 图 3 示出可通过二维码识别设备读取的图片的示意图;
- [102] 图 4 示出将第一图片置于二维码图片中心的示意图;
- 5 [103] 图 5 示出根据本说明书实施例的一种提供二维码的方法的流程图;
- [104] 图 6 示出根据本说明书实施例的一种验证二维码的方法流程图;
- [105] 图 7 示出根据本说明书实施例的服务器与第一用户终端、第二用户终端之间的交互图;
- [106] 图 8 示出根据本说明书实施例的一种验证二维码的方法;
- 10 [107] 图 9 示出根据本说明书实施例的一种提供二维码的装置 900;
- [108] 图 10 示出根据本说明书实施例的一种提供二维码的装置 1000;
- [109] 图 11 示出根据本说明书实施例的一种验证二维码的装置 1100;
- [110] 图 12 示出根据本说明书实施例的一种验证二维码的装置 1200。

具体实施方式

- 15 [111] 下面将结合附图描述本说明书实施例。
- [112] 图 1 示出根据本说明书实施例的基于二维码的业务系统 100 的示意图。如图 1 所示, 系统 100 可以包括服务器 11、网络 12、手机 13 和计算机 14 等。系统 100 例如用于进行商户与消费者之间的交易业务。服务器 11 可以为包含一独立主机的物理服务器, 或者该服务器 11 可以为主机集群承载的虚拟服务器; 该服务器 11 可以承载例如所
- 20 述交易业务的业务平台, 比如该业务平台可以为支付平台。手机 13 例如为消费者使用的终端, 该手机 13 上运行有客户端, 该客户端例如可以实现与消费者相关的业务功能, 当然, 除了手机 13 之外, 消费者还可以采用计算机、平板设备、笔记本电脑、掌上电脑、可穿戴设备(如智能眼镜、智能手表等)等其他类型的终端设备, 本说明书并不对此进行限制。计算机 14 可以为商户使用的终端设备, 该计算机 14 上运行有客户端 2,
- 25 该客户端 2 可以实现例如与商户相关的业务功能; 当然, 除了计算机 14 之外, 商户还可以采用手机、平板设备、笔记本电脑、掌上电脑、可穿戴设备(如智能眼镜、智能手表等)等其他类型的终端设备, 本说明书并不对此进行限制。手机 13、计算机 14 与服

务器 11 之间通过网络 12 进行交互,所述网络 12 可以包括多种类型的有线或无线网络,比如,该网络 12 可以包括公共交换电话网络(Public Switched Telephone Network, PSTN)和因特网。

[113] 根据本说明书实施例,在生成二维码的阶段,计算机 14 向服务器 11 发送生成
5 二维码的请求,该请求包括商户的用户标识。服务器 11 获取与该用户标识对应的第一
图片,在服务器本地将其关联地存储,并对第一图片和业务数据的组合进行加密,以获
取加密数据,然后,基于加密数据生成二维码,并将所述第一图片叠加在所述二维码上,
从而生成最终的业务码,并将该业务码发送给计算机 14。在二维码验证阶段,例如,消
费者通过扫描商户的二维码准备进行支付,在该情况中,手机 13 扫描上述业务码,读
10 取该业务码,并将其发送给服务器 11。服务器 11 基于该业务码获取二维码和第一图片。
然后,服务器 11 对二维码解码,获取二维码的内容数据,并通过预定解密方法对该内
容数据解密,从而获取业务数据和第二图片。服务器 11 比较第一图片与第二图片,在
第一图片与第二图片相似度较低的情况中,确定验证不通过,从而终止交易。在第一图
片与第二图片相似度高于预定阈值的情况中,服务器 11 基于业务数据中包括的用户标
15 识,获取与该用户标识对应的第三图片,并比较第三图片与第一图片是否一致。在第三
图片与第一图片不一致的情况中,确定验证不通过,从而终止交易,在第三图片与第一
图片一致的情况中,确定验证通过,继续交易业务。

[114] 图 1 所示的系统 100 和相关的描述只是示意性地,例如,系统 100 可包括多个
商户的终端、多个消费者的终端。另外,所述服务器不限于对应于支付平台,例如还可
20 以对应于社交平台、下载平台等,其中,在社交平台中,例如在用户收听公众号时,通
过根据本说明书实施例的系统可避免由于二维码被替换造成的粉丝截流,在下载平台中,
通过根据本说明书实施例的系统可避免由于二维码被替换造成的下载截流等等。

[115] 图 2 示出根据本说明书实施例的一种提供二维码的方法流程图,包括:

[116] 在步骤 S202,从第一用户的终端接收二维码生成请求,所述请求中包括该二维
25 码对应的业务数据,其中,所述业务数据包括所述第一用户的用户标识;

[117] 在步骤 S204,获取第一图片以与所述用户标识相对应,其中,所述第一图片为
肉眼可识别图片;

[118] 在步骤 S206,存储所述用户标识与所述第一图片的关联关系;

[119] 在步骤 S208,基于所述第一图片与所述业务数据生成二维码;以及

[120] 在步骤 S210, 将所述二维码和所述第一图片提供给所述第一用户。

[121] 首先, 在步骤 S202, 从第一用户的终端接收二维码生成请求, 所述请求中包括该二维码对应的业务数据, 其中, 所述业务数据包括所述第一用户的用户标识。

[122] 如上文所述, 该方法例如在业务平台的服务器中执行, 该业务平台例如为支付平台 (如支付宝平台), 第一用户例如为商户, 其终端可以为计算机、手机等等。商户例如希望将其支付宝账户生成二维码以便于消费者进行支付, 从而, 商户向服务器发送二维码生成请求, 并在该请求中包括自己的支付宝账户。在一个实施例中, 商户例如希望对其出售的每个商品生成一个二维码, 以便于消费者在挑选商品时可以自动购买, 在该情况中, 商户向服务器发送的二维码生成请求中, 除了包括其支付宝账户之外, 还可以包括商品名称、商品价格等业务数据。可以理解, 所述业务平台不限于支付平台, 而对应于不同的业务平台, 二维码生成请求中包括的业务数据也相应地不同, 例如, 在下载平台中, 业务数据中可能包括下载 APP 的名称、APP 价格等业务数据。

[123] 在步骤 S204, 获取第一图片以与所述用户标识相对应, 其中, 所述第一图片为肉眼可识别图片。

[124] 所述第一图片必须是肉眼可识别的, 例如, 该图片中可包括较清晰的图案、文字、数字、符号及其组合等。所述图案例如可以为心形图案、计算机图案等。所述文字可以为各种语言, 如汉语、英语等。所述数字可以为阿拉伯数字、罗马数字等等。所述符号例如包括标点符号、表情符号、运算符号等等。另外, 该图片中还可以包括不同的颜色以用于图片识别。通过使得第一图片具有可识别性, 在后续的二维码使用中, 才能首先由二维码使用者基于该第一图片由肉眼识别该二维码的真假。

[125] 在一个实施例中, 所述第一图片可通过二维码识别设备读取。所述二维码识别设备例如为手机、扫码枪等。在例如扫码枪的情况中, 扫码枪通过其中的光电装置对二维码进行扫码, 从而将该二维码转换为二进制的字符串 (即 01 串)。图 3 示出可通过二维码识别设备读取的图片的示意图。如图 3 所示, 图中示出的六个图案都是基于二维码的格式生成, 即, 其中的边缘或内部由多个方块构成, 该方块与二维码图形中的一位的大小相同, 从而使得扫码枪在扫码该图片时, 可与二维码同时地将其识别为二进制字符串。在一个实施例中, 识别设备中可包括颜色识别装置, 从而可将彩色的第一图片识别为带颜色信息的二进制字符串。可以理解, 所述第一图片不必须可通过二维码识别设备读取, 例如, 当通过手机扫描该第一图片之后, 可通过图像识别设备、装置、单元等识别该第一图片。

- [126] 在一个实施例中，所述第一图片将在后续步骤中被置于所述二维码的内部（例如中心处）。在该情况中，所述第一图片的面积基于所述二维码的纠错级别确定。例如，二维码的纠错级别越大，该第一图片的面积可以越大。从而，当将该第一图片置于二维码中心处的情况下，仍可通过纠错码识别出该二维码的完整数据。
- 5 [127] 在一个实施例中，所述用户标识与所述第一图片唯一对应，例如商户在全国多个城市开有分店，该商户的支付二维码将在多个城市使用，通过使得用户标识与第一图片唯一对应，可确保该二维码在任何城市的安全性。在一个实施例中，所述第一图片在所述二维码的使用地域范围中与所述用户标识唯一对应。例如，商户只是在一个城市（例如北京）进行营业，即，其二维码只在北京使用，并且在北京范围内，商户的用户标识
- 10 与第一图片是唯一对应的。而在地，例如在杭州，即使存在另一个用户标识，其对应的图片与该第一图片相同，其获知北京的该商户的第一图片与其对应图片相同、并用自己二维码对该商户的二维码进行套码的概率将会非常低。
- [128] 在一个实施例中，可预先建立图库，该图库中包括数量足够大的用于验证的图片，例如图片数量的量级为十万量级、百万量级等等。当需要生成二维码、并需要获取
- 15 与用户标识对应的图片时，在一个实施例中，可从该图库中获取第一图片，并在获取该第一图片中，在图库中将该第一图片标记为不可用，从而避免对该第一图片的重复使用。在一个实施例中，可从该图库中随机获取第一图片，由于该图库的图片数量巨大，从而，图片的重复获取概率非常低，从而确保了该方法的安全性。
- [129] 在本说明书实施例中，不限于从图库中获取第一图片，例如，可通过基于预定
- 20 规则现场生成第一图片，可通过由第一用户自身提交图片，从而获取第一图片等等。在这些情况中，只要确保第一图片相对于不同用户标识的重复获取率低于预定阈值即可，从而可保证该方法的安全性。
- [130] 在一个实施例中，所述第一图片的图像数据量小于第二预定值。由于根据该方法的后续步骤，通过对该第一图片与业务数据的组合进行加密，获取加密数据，并对该
- 25 加密数据进行编码，从而获取二维码，从而基于二维码可表示的最大位数、加密方法、以及业务数据预留量，可确定该第一图片的数据量的最大值，并将该第一图片图像数据量限定为小于等于该最大值时。另外，将第一图片图像数据量限定为小于等于预定值，也有利于在传输该第一图片时，节省数据传输成本。在一个实施例中，在第一图片的数据量较大的情况中，可首先对第一图片进行压缩，然后对该压缩后的第一图片与业务数
- 30 据的组合进行加密。

- [131] 在步骤 S206, 存储所述用户标识与所述第一图片的关联关系。在一个实施例中, 将用户标识与第一图片记录到数据库中, 以用于后续的验证。所述用户标识例如为用户邮箱地址, 在第一图片例如为图 3 所示的图片的情况下, 其可用二进制字符串表示并存储到数据库中。在一个实施例中, 可将用户标识与第一图片的标识记录到数据库中, 例如, 第一图片为数据量较大图片, 在该情况中, 可对图库中的图片进行编号, 并在数据库中仅记录第一图片的编号及对应的用户标识, 在进行二维码验证时, 可根据图片编号在图库中获取对应的图片。
- [132] 在步骤 S208, 基于所述第一图片与所述业务数据生成二维码。
- [133] 在一个实施例中, 基于所述第一图片与所述业务数据生成二维码包括, 通过预定加密方法对所述第一图片与所述业务数据的组合进行加密以获取加密数据, 并基于所述加密数据生成二维码。
- [134] 第一图片可表示为一个 01 字符矩阵, 从而可基于该字符矩阵获取 01 字符串。所述业务数据例如为第一用户的用户标识, 例如为第一用户的电子邮箱地址、手机号码等。从而, 第一图片与业务数据的组合可以为数字的组合, 也可以为数字与字母、符号的组合等等。本说明书对于所述组合的方式并不进行限制, 例如可将用户标识置于第一图片对应的字符串之前或之后或中间等等, 只要在后续进行二维码验证时可以相应地将其拆分开即可。所述加密方式可以为对称加密、非对称加密等等, 本说明书并不对此进行限制。在经过该加密之后获取的加密数据也可以为数字的组合、数字与字母、符号的组合等等。然后, 基于所述加密数据, 通过预定版本的二维码的编码规则, 对该加密数据进行编码, 从而获取二维码。该二维码以图片的格式存储。
- [135] 在本说明书实施例中, 基于所述第一图片与所述业务数据生成二维码不限于基于其的组合的加密数据生成二维码, 例如, 可基于所述组合直接生成二维码, 基于第一图片的加密数据与业务数据的组合生成二维码、基于第一图片的哈希值与业务数据的组合生成二维码等等。
- [136] 在步骤 S210, 将所述二维码和所述第一图片提供给所述第一用户。
- [137] 在一个实施例中, 在生成二维码之后, 将所述二维码和所述第一图片发送给所述第一用户的终端。在一个实施例中, 在获取二维码之后, 将第一图片与二维码图片叠加到一起以获取业务码, 从而向第一用户的终端发送业务码, 以同时发送所述第一图片和二维码。在一个实施例中, 将第一图片置于二维码内部, 例如, 将第一图片置于二

码图片的中心，即类似于传统二维码的 logo 区的位置，图 4 示出将第一图片置于二维码图片中心的示意图。如图 4 所示，图中示出两个根据本说明书实施例的业务码。这两个业务码中心的图案具有可辨别性，因此可肉眼识别出这两个业务码对应于不同的用户标识。而如图中所示，业务码中心位置为第一图片所在位置，该位置即为根据本说明书实
5 施例的验证区，在该业务码验证区周围为数据区。在该情况中，如前文所述，需基于二
维码的纠错级别确定该第一图片的图片面积。该第一图片不限于置于二维码图片的内部，
例如，该第一图片可置于二维码图片的外部，例如可置于二维码图片的一边之外，可置
于二维码图片的四边之外等等，本说明书并不对此进行限制。在将第一图片置于二维码
图片外部的情况中，对第一图片的尺寸不作限制，一般可将第一图片的尺寸设置为方便
10 二维码扫描设备在一次扫描中同时扫描所述第一图片和所述二维码。

[138] 可以理解，所述第一图片和所述二维码图片不限于一次传输，也可以在两次传
输中分别向第一用户的终端发送第一图片和二维码图片。例如，可以先发送第一图片，
再发送二维码图片等等。另外，本说明书实施例不限于由服务器将所述第一图片和所述
二维码图片发送给第一用户的终端，例如，可由第一用户的终端从服务器读取所述二维
15 码图片和第一图片等等。

[139] 第一用户在从服务器接收所述二维码和第一图片之后，可对其进行打印，并张
贴出来，以方便其他用户进行扫码。

[140] 图 5 示出根据本说明书实施例的一种提供二维码的方法的流程图，包括：

[141] 在步骤 S502，从第一用户的终端接收二维码生成请求，所述请求中包括该二维
20 码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；

[142] 在步骤 S504，获取第一图片以与所述用户标识相对应，其中，所述第一图片为
肉眼可识别图片；

[143] 在步骤 S506，存储所述用户标识与所述第一图片的关联关系；

[144] 在步骤 S508，基于所述业务数据生成二维码；以及

25 [145] 在步骤 S510，将所述二维码和所述第一图片提供给所述第一用户。

[146] 其中，步骤 S502-S506 和 S510 可参考上述对步骤 S202-S206 和 S210 的具体描
述，在此不再赘述。图 5 所示方法与图 2 所示方法不同在于，在步骤 S508，基于所述
业务数据生成二维码。例如，所述业务数据为第一用户的用户标识，在该步骤中，可基
于该用户标识生成二维码，或者基于该用户标识的加密数据生成二维码等等。同样地，

所述业务数据不限于仅包括用户标识，而可以例如商品金额等其它业务数据。在该情况中，对第一图片的图像数据量不再有限制。

[147] 图 6 示出根据本说明书实施例的一种验证二维码的方法流程图，包括：

[148] 在步骤 S602，从第二用户的终端接收二维码信息和第一图片；

5 [149] 在步骤 S604，基于所述二维码信息，获取二维码的内容数据；

[150] 在步骤 S606，基于所述二维码的内容数据，获取业务数据和第二图片信息；

[151] 在步骤 S608，基于所述第一图片和所述第二图片信息，确定所述第一图片与所述第二图片的相似度；以及

[152] 在步骤 S610，在所述相似度低于预定阈值时，确定所述验证不通过。

10 [153] 首先，在步骤 S602，从第二用户的终端接收二维码信息和第一图片。该方法在业务平台（例如支付平台）的服务器中执行，所述第二用户例如为消费者，其通过使用自己的二维码识别设备（例如手机）扫描商户的业务码而即将通过该支付平台进行支付业务。该第二用户在扫码之前可观察第一图片，以确定该第一图片是否为商户的预先公示的验证图片，由于第一图片为肉眼可识别图片，第二用户可容易地进行该确定。例如，
15 第一图片叠加在二维码的中心位置，第二用户通过观察二维码的中心位置的第一图片，确定该第一图片是否是商户的验证图片。也就是说，第二用户在确定第一图片是商户的验证图片之后，对该业务码进行扫码。另一方面，商户也可以通过肉眼检测其业务码中的图片是否为其验证图片，以确定该业务码是否被他人替换。

[154] 在一个实施例中，如上文所述，在该二维码和第一图片为叠加在一起的业务码
20 的情况中，第二用户通过扫描业务码，将该业务码读取为二进制数据串，并将该二进制数据串发送给服务器。其中，根据预先设定好的位置，所述二进制数据串中预定位置的数据为对应于第一图片的数据，其它位置为对应于二维码的数据。

[155] 在一个实施例中，用户二维码识别设备中配置有对二维码进行解码的硬件或软件，从而，用户在将上述业务码读取为二进制数据串之后，除了如上所述获取对应于第一
25 图片的数据之外，还通过解码装置对其中对应于二维码的数据进行解码，从而获取该二维码对应的内容数据。

[156] 另外，如上文所述，所述二维码信息和所述第一图片不限定为由第二用户设备在一次中发送。在所述二维码信息和所述第一图片叠加为业务码的情况中，第二用户设

备在读取二进制字符串并获取对应于第一图片的数据串之后，可先将第一图片（对应的数据串）发送给服务器，然后在对二维码解码之后，将二维码的内容信息再发送给服务器。在所述二维码和所述第一图片未叠加在一起，第二用户设备分两次分别扫描二维码和第一图片的情况中，可先后在每次扫描后向服务器发送二维码信息和第一图片。

5 [157] 在步骤 S604，基于所述二维码信息，获取二维码的内容数据。

[158] 如上文所述，在一个实施例中，第二用户的设备扫描业务码，并读取该业务码对应的二进制字符串，并将该字符串发送给服务器。在该情况中，二维码信息为所述字符串中对应于二维码部分的字符串。服务器基于二维码中的纠错码对二维码进行解码，获取二维码完整的内容数据。

10 [159] 在一个实施例中，第二用户的设备中包括解码装置，并通过对扫描获取的二维码进行解码，从而获取二维码的内容数据，并将该二维码的内容数据发送给服务器，即，所述二维码信息包括二维码的内容数据。从而，服务器可直接从接收的二维码信息中获取二维码的内容数据，而不需要另外解码。

[160] 在步骤 S606，基于所述二维码的内容数据，获取业务数据和第二图片信息。

15 [161] 在一个实施例中，基于所述二维码的内容数据，获取业务数据和第二图片信息包括，通过预定解密方法对所述二维码的内容数据进行解密，从而获取业务数据和第二图片。

[162] 如上文参考图 2 所述，服务器在生成二维码时，基于加密数据生成二维码，而加密数据是通过对业务数据和第二图片的组合进行加密所获取。因此，在获取二维码内容数据之后，可相应地对该内容数据进行解密。例如，在通过对称加密方法进行加密的情况中，可通过与加密时相同的密钥对该内容数据进行解密。在通过非对称加密方法进行加密的情况中，可通过预先设定好的另一密钥对该内容数据进行解密。在解密之后，根据业务数据与第二图片在加密时的组合形式，对解密数据进行拆分，从而获取业务数据和第二图片。这里，第二图片即第二图片的数据表示，通常为二进制字符矩阵，其从
20 解密数据中的与第二图片对应的数据串获取，例如，在对应于第二图片的顺序排列的二进制字符串中，以预定数目的连续字符为一行获取矩阵的多行，从而获取与第二图片对应的二进制字符矩阵。另外，如上文所述，所述业务数据为明文数据，例如，在支付平台的场景中，其对应于用户（例如第一用户）的账户。

25 [163] 可以理解，基于所述二维码的内容数据，获取业务数据和第二图片信息的方式

不限于上述解密的方式，其具体方式取决于所获取的二维码的内容数据的形式。例如，所述二维码的内容数据为明文的业务数据和第二图片的组合，则可直接获取业务数据和第二图片。例如，所述二维码的内容数据为业务数据的加密数据与第二图片的组合，则可通过对业务数据解密获取业务数据和第二图片。例如，所述二维码的内容数据为业务数据与第二图片的哈希值的组合，则可直接获取业务数据和第二图片的哈希值（即第二图片信息），等等。

[164] 在步骤 S608，基于所述第一图片和所述第二图片信息，确定所述第一图片与所述第二图片的相似度。

[165] 在一个实施例中，第二图片信息为第二图片本身，在第一图片为图 3 所示的图片的情况下，即，第二用户的识别设备在读取二维码的同时可读取第一图片，在二维码未被替换的情况下，第二图片例如为通过对二维码与第一图片的组合进行加密、由设备扫码、解密、以及拆分所获取的图片，因此，该第二图片与第一图片应基本相同，其中，设备扫码时可能会存在轻微误差，以及在加密并解密之后，由于加密方法的不同，可能会造成轻微的误差。在该情况下，第一图片与第二图片的相似度可通过各种相似度计算方法基于第一图片与第二图片的数据表示（例如矩阵）计算其相似度，并且其相似度应较高。所述相似度包括欧式距离、明氏距离、余弦相似度等。

[166] 在一个实施例中，第二图片信息为第二图片本身，在第一图片不能通过二维码识别设备直接读取而是通过例如图像识别装置进行识别的情况下，在二维码未被替换的情况下，由于通过图像识别获取的图片的清晰度、颜色、亮度等都会存在偏差，因此，第一图片与第二图片（第二图片如上段中所述获取）的相似度应低于上一种情况中二者的相似度。在该情况下，可以同样地通过各种相似度计算方法基于第一图片与第二图片的数据表示计算其相似度，也可以基于第一图片与第二图片的图片特征、内容特征计算其相似度等等。

[167] 在一个实施例中，在上述二维码的内容数据为业务数据与第二图片的哈希值的组合的情况下，即，第二图片信息为第二图片的哈希值，可通过对第一图片进行同样的哈希计算，以获取第一图片的哈希值，并基于第一图片的哈希值与第二图片的哈希值，计算第一图片与第二图片的相似度。

[168] 在步骤 S610，在所述相似度低于预定阈值时，确定所述验证不通过。

[169] 可根据不同类型的图片，设定阈值的大小。例如，在上述第一图片为图 3 所示

图片的情况中，在二维码未被替换的情况中，第一图片与第二图片的相似度应非常高，因此，可将该类型图片的情况下的预定阈值设定为较高，例如相似度阈值为 90%，在低于 90% 时，即确定验证不通过。例如，在上述第一图片是通过图像识别装置进行图像识别而获取的情况中，相应地，可将预定阈值设置为低于上述情况中的阈值，例如设置为 80%。

[170] 在例如支付场景中，例如第二用户通过扫描业务码准备向第一用户进行支付。如前文所述，第一用户已经确认了业务码中的第一图片为第一用户预先公示的其验证图片，如果他人（如第三用户）将该业务码中的二维码部分简单地替换成他自己的二维码，即包括第三用户的用户标识，则服务器通过基于前述步骤 S602-S606 从第三用户的二维码获取第二图片之后，第二图片与第一图片必然差别很大，即第一图片与第二图片的相似度低于预定阈值，从而可确定验证不通过，以制止这种套码行为。从而，通过简单地比较第一图片和第二图片就可以初步制止这种套码行为，而省去了后续地查找数据库的步骤，节省了时间成本。

[171] 在上述场景中，在确定验证不通过之后，可终止支付业务，另外，可通知第二用户，该二维码已被替换。在一个实施例中，还可以通过第一图片获取第一图片对应的商户账户，并通知该商户其二维码被他人替换。在一个实施例中，还可以在平台中发出公告，以提醒其他用户注意类似风险。

[172] 在一个实施例中，在上述解密获取的业务数据中包括第三用户的用户标识，例如，在支付场景中，业务数据中包括的用户标识为将用于收款的账户。在所述第一图片与所述第二图片相似度高于预定阈值的情况中，基于预存的用户标识与图片的关联关系，获取与所述第三用户的用户标识对应的第三图片；以及在所述第一图片与所述第三图片不一致的情况中，确定所述验证不通过。根据上述参考图 2 的描述，平台服务器在生成每个二维码时都会获取与相应用户标识对应的图片，并将其关联关系存储在服务器中，例如存储在数据库中。因此，在从业务数据中获取第三用户的用户标识之后，可从数据库中查找出与该第三用户的用户标识对应的第三图片。

[173] 在一种套码场景中，第三用户破解了所述加密算法，其通过所述加密算法将自己的账户与第一图片的组合进行加密生成二维码并叠加第一图片生成非法的业务码，在该情况中，第二用户通过肉眼识别第一图片为第一用户的验证图片，并且服务器也确定第一图片与第二图片是相同的。但是服务器在获取第三用户的账户之后，搜索出与第三用户对应的第三图片，并确定该第三图片与第一图片不一致，从而可确定验证不通过，

制止该种套码行为，并终止支付业务。

[174] 在一个实施例中，例如在第二用户打算通过该二维码向第一用户进行支付的场景中，在该二维码未被替换的情况中，该第三用户即第一用户，即，第三图片与第一图片都是第一用户对应的图片，从而是一致的。从而，在第一图片与第三图片一致的情况中，可确定验证通过，并将业务数据发送给第二用户的终端，以继续进行所述支付业务。

[175] 图 7 示出根据本说明书实施例的服务器与第一用户终端、第二用户终端之间的交互图。如图 7 所示，第一阶段为生成二维码的阶段。首先，第一用户终端在步骤 701 向服务器发送二维码生成请求，该请求中包括二维码对应的业务数据，在该业务数据中包括第一用户的用户标识。服务器在接收该请求之后，在步骤 702 获取第一图片，以与第一用户的用户标识相对应，并在步骤 703 将第一图片与该用户标识的关联关系存储起来。然后，在步骤 704，服务器对用户标识与第一图片的组合进行加密，以生成加密数据，并在步骤 705，基于加密数据生成二维码。之后，服务器在步骤 706 将二维码和第一图片发送给第一用户的终端以供第一用户使用。在一个实施例中，服务器将第一图片叠加在二维码的中心形成业务码，并将该业务码发给第一用户终端。第一用户终端在接收该业务码之后，在步骤 707 将业务码打印出来，例如张贴在收银台处以供消费者扫描支付。

[176] 如图 7 所示，第二阶段为验证二维码的阶段。第二用户在步骤 708 使用其终端（如手机）扫描上述业务码，从而获取二维码信息和第一图片，并在步骤 709 将其发送给服务器。服务器在接收所述二维码信息和第一图片之后，在步骤 710 获取二维码的内容数据，在步骤 711，对该内容数据解密，获取业务数据和第二图片。在步骤 712，服务器确定第一图片与第二图片的相似度，在步骤 713，当相似度低于预定阈值时，确定验证不通过。在步骤 714-715，在确定验证不通过之后，服务器可分别通知第一用户终端和第二用户终端，以提醒其警惕套码风险，另外，服务器也可以在平台发出公告，以提醒其他用户警惕套码风险。在步骤 716，在相似度高于预定阈值的情况中，服务器获取与业务数据中包括的用户标识关联的第三图片，在步骤 717，确定第一图片与第三图片是否一致，如果不一致，则在步骤 718 确定验证不通过，并与上述类似地在步骤 719-720 通知第一用户和第二用户，如果一致，则在步骤 721 确定验证通过，并在步骤 722 向第二用户终端发送业务数据，以继续后续的业务。

[177] 图 8 示出根据本说明书实施例的一种验证二维码的方法，包括：

[178] 在步骤 S802，从第二用户的终端接收二维码信息和第一图片；

- [179] 在步骤 S804, 基于所述二维码信息, 获取二维码的内容数据;
- [180] 在步骤 S806, 基于所述二维码的内容数据, 获取业务数据, 其中, 所述业务数据中包括第三用户的用户标识;
- [181] 在步骤 S808, 基于预存的用户标识与图片的关联关系, 获取与所述第三用户的
5 用户标识对应的第三图片;
- [182] 在步骤 S810, 确定所述第一图片与所述第三图片是否一致; 以及
- [183] 在步骤 S812, 在所述第一图片与所述第三图片不一致的情况中, 确定所述验证不通过。
- [184] 其中, 步骤 S802-S804、S808-S812 可参考上文中对图 6 相应步骤的具体描述,
10 在此不再赘述。在步骤 S806, 基于所述二维码的内容数据, 获取业务数据, 其中, 所述业务数据中包括第三用户的用户标识。在一个实施例中, 所述二维码的内容数据为业务数据明文, 则可直接获取该业务数据。在一个实施例中, 所述二维码的内容数据为业务数据的加密数据, 则通过预定解密方法对该加密数据进行解密, 从而可获取相应的业务数据。
- 15 [185] 所述方法还包括: 在所述第一图片与所述第三图片一致的情况中, 确定所述验证通过; 以及将所述业务数据发送给所述第二用户的终端。
- [186] 图 9 示出根据本说明书实施例的一种提供二维码的装置 900, 包括:
- [187] 接收单元 91, 配置为, 从第一用户的终端接收二维码生成请求, 所述请求中包括该二维码对应的业务数据, 其中, 所述业务数据包括所述第一用户的用户标识;
- 20 [188] 获取单元 92, 配置为, 获取第一图片以与所述用户标识相对应, 其中, 所述第一图片为肉眼可识别图片;
- [189] 存储单元 93, 配置为, 存储所述用户标识与所述第一图片的关联关系;
- [190] 生成单元 94, 配置为, 基于所述第一图片与所述业务数据生成二维码; 以及
- [191] 提供单元 95, 配置为, 将所述二维码和所述第一图片提供给所述第一用户。
- 25 [192] 在一个实施例中, 所述提供单元 95 还包括, 叠加子单元 951, 配置为, 通过叠加所述第一图片和所述二维码获取业务码, 以及, 提供子单元 952, 配置为, 将所述业务码发送给所述第一用户。

- [193] 在一个实施例中,所述获取单元 92 还配置为,从预先建立的图库中获取与所述用户标识对应的第一图片,其中,所述图库包括数量多于预定值的图片。
- [194] 在一个实施例中,所述装置还包括标记单元 96,配置为,在从预先建立的图库中获取与所述用户标识对应的第一图片之后,在所述图库中对所述第一图片进行标记。
- 5 [195] 在一个实施例中,所述获取单元 92 还配置为,从预先建立的图库中随机获取与
所述用户标识对应的第一图片。
- [196] 图 10 示出根据本说明书实施例的一种提供二维码的装置 1000,包括:
- [197] 接收单元 101,配置为,从第一用户的终端接收二维码生成请求,所述请求中包括该二维码对应的业务数据,其中,所述业务数据包括所述第一用户的用户标识;
- 10 [198] 获取单元 102,配置为,获取第一图片以与所述用户标识相对应,其中,所述第一
图片为肉眼可识别图片;
- [199] 存储单元 103,配置为,存储所述用户标识与所述第一图片的关联关系;
- [200] 生成单元 104,配置为,基于所述业务数据生成二维码;以及
- [201] 提供单元 105,配置为,将所述二维码和所述第一图片提供给所述第一用户。
- 15 [202] 图 11 示出根据本说明书实施例的一种验证二维码的装置 1100,包括:
- [203] 接收单元 1101,配置为,从第二用户的终端接收二维码信息和第一图片;
- [204] 第一获取单元 1102,配置为,基于所述二维码信息,获取二维码的内容数据;
- [205] 第二获取单元 1103,配置为,基于所述二维码的内容数据,获取业务数据和第
二图片信息;
- 20 [206] 第一确定单元 1104,配置为,基于所述第一图片和所述第二图片信息,确定所
述第一图片与所述第二图片的相似度;以及
- [207] 第二确定单元 1105,配置为,在所述相似度低于预定阈值时,确定所述验证不
通过。
- [208] 在一个实施例中,所述第二获取单元 1103 还配置为,通过预定解密方法对所述
25 二维码的内容数据进行解密,从而获取业务数据和第二图片。
- [209] 在一个实施例中,所述接收单元 1101 还配置为,从第二用户的终端接收业务码,
其中,所述业务码中包括叠加的二维码和所述第一图片。

[210] 在一个实施例中, 所述业务数据包括第三用户的用户标识, 所述装置还包括:

[211] 第三获取单元 1106, 配置为, 在所述第一图片与所述第二图片相似度高于预定阈值的情况中, 基于预存的用户标识与图片的关联关系, 获取与所述第三用户的用户标识对应的第三图片;

5 [212] 第三确定单元 1107, 配置为, 确定所述第一图片与所述第三图片是否一致; 以及

[213] 第四确定单元 1108, 配置为, 在所述第一图片与所述第三图片不一致的情况中, 确定所述验证不通过。

[214] 在一个实施例中, 所述装置还包括:

10 [215] 第五确定单元 1109, 配置为, 在所述第一图片与所述第三图片一致的情况中, 确定所述验证通过; 以及

[216] 发送单元 1110, 配置为, 将所述业务数据发送给所述第二用户的终端。

[217] 图 12 示出根据本说明书实施例的一种验证二维码的装置 1200, 包括:

[218] 接收单元 121, 配置为, 从第二用户的终端接收二维码信息和第一图片;

15 [219] 第一获取单元 122, 配置为, 基于所述二维码信息, 获取二维码的内容数据;

[220] 第二获取单元 123, 配置为, 基于所述二维码的内容数据, 获取业务数据, 其中, 所述业务数据中包括第三用户的用户标识;

[221] 第三获取单元 124, 配置为, 基于预存的用户标识与图片的关联关系, 获取与所述第三用户的用户标识对应的第三图片;

20 [222] 第一确定单元 125, 配置为, 确定所述第一图片与所述第三图片是否一致; 以及

[223] 第二确定单元 126, 配置为, 在所述第一图片与所述第三图片不一致的情况中, 确定所述验证不通过。

[224] 在一个实施例中, 所述装置还包括:

[225] 第三确定单元 127, 配置为, 在所述第一图片与所述第三图片一致的情况中, 确定所述验证通过; 以及

25

[226] 发送单元 128, 配置为, 将所述业务数据发送给所述第二用户的终端。

[227] 本说明书另一方面提供一种计算设备, 包括存储器和处理器, 其特征在于, 所

述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现上述任一种方法。

[228] 根据本说明书实施例的二维码方案与传统的二维码相比，增加“验证图片”，验证图片所携带和展示的信息与二维码主体呈基本唯一对应的关系，并且验证图片具有明显区分度，从而使得：当二维码整体被替换(主体+验证图片)时，用户（例如商户或消费者）很容易肉眼发现。当二维码主体被替换，而验证图片保留时，整体的流程会被服务器端判断为校验不通过，流程中断，从而避免资金损失或其他风险。

[229] 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。

[230] 上述对本说明书特定实施例进行了描述。其它实施例在所附权利要求书的范围内。在一些情况下，在权利要求书中记载的动作或步骤可以按照不同于其中的顺序来执行并且仍然可以实现期望的结果。另外，在附图中描绘的过程不一定要求示出的特定顺序或者连续顺序才能实现期望的结果。在某些实施方式中，多任务处理和并行处理也是可以的或者可能是有利的。

[231] 本领域普通技术人员应该还可以进一步意识到，结合本文中所公开的实施例描述的各示例的单元及算法步骤，能够以电子硬件、计算机软件或者二者的结合来实现，为了清楚地说明硬件和软件的可互换性，在上述说明中已经按照功能一般性地描述了各示例的组成及步骤。这些功能究竟以硬件还是软件方式来执轨道，取决于技术方案的具体应用和设计约束条件。本领域普通技术人员可以对每个特定的应用来使用不同方法来实现所描述的功能，但是这种实现不应认为超出本申请的范围。

[232] 结合本文中所公开的实施例描述的方法或算法的步骤可以用硬件、处理器执轨道的软件模块，或者二者的结合来实施。软件模块可以置于随机存储器(RAM)、内存、只读存储器(ROM)、电可编程ROM、电可擦除可编程ROM、寄存器、硬盘、可移动磁盘、CD-ROM、或技术领域内所公知的任意其它形式的存储介质中。

[233] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进

等，均应包含在本发明的保护范围之内。

权利要求书

1. 一种提供二维码的方法，包括：

从第一用户的终端接收二维码生成请求，所述请求中包括该二维码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；
- 5 获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

存储所述用户标识与所述第一图片的关联关系；

基于所述业务数据生成二维码；以及

将所述二维码和所述第一图片提供给所述第一用户。
- 10 2. 一种提供二维码的方法，包括：

从第一用户的终端接收二维码生成请求，所述请求中包括该二维码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；

获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

存储所述用户标识与所述第一图片的关联关系；

基于所述第一图片与所述业务数据生成二维码；以及
- 15 将所述二维码和所述第一图片提供给所述第一用户。
3. 根据权利要求 1 或 2 所述的方法，其中将所述二维码和所述第一图片提供给所述第一用户包括，通过叠加所述第一图片和所述二维码获取业务码，以及，将所述业务码提供给所述第一用户。
- 20 4. 根据权利要求 3 所述的方法，其中所述第一图片为二维码识别设备能够读取的图片。
5. 根据权利要求 3 所述的方法，其中，所述第一图片位于所述二维码内部。
6. 根据权利要求 5 所述的方法，其中，所述第一图片的面积基于所述二维码的纠错级别确定。
7. 根据权利要求 1 或 2 所述的方法，其中，所述第一图片包括以下至少一种内容：

25 图案、文字、数字、符号。
8. 根据权利要求 1 或 2 所述的方法，其中，所述第一图片的用于对应于其他用户标识的重复获取率低于第一预定值。
9. 根据权利要求 8 所述的方法，其中，所述用户标识与所述第一图片唯一对应。
10. 根据权利要求 8 所述的方法，其中，获取与所述用户标识对应的第一图片包括，

30 从预先建立的图库中获取与所述用户标识对应的第一图片，其中，所述图库包括数量多于预定值的图片。

11. 根据权利要求 10 所述的方法, 还包括, 在从预先建立的图库中获取与所述用户标识对应的第一图片之后, 在所述图库中对所述第一图片进行标记。

12. 根据权利要求 10 或 11 所述的方法, 其中, 从预先建立的图库中获取与所述用户标识对应的第一图片包括, 从预先建立的图库中随机获取与所述用户标识对应的第一
5 图片。

13. 根据权利要求 2 所述的方法, 其中, 所述第一图片的图像数据量小于等于第二预定值。

14. 根据权利要求 2 所述的方法, 其中, 基于所述第一图片与所述业务数据生成二维码包括, 通过预定加密方法对所述第一图片与所述业务数据的组合进行加密以获取加
10 密数据, 并基于所述加密数据生成二维码。

15. 一种验证二维码的方法, 包括:

从第二用户的终端接收二维码信息和第一图片;

基于所述二维码信息, 获取二维码的内容数据;

基于所述二维码的内容数据, 获取业务数据, 其中, 所述业务数据中包括第三用户
15 的用户标识;

基于预存的用户标识与图片的关联关系, 获取与所述第三用户的用户标识对应的第三图片;

确定所述第一图片与所述第三图片是否一致; 以及

在所述第一图片与所述第三图片不一致的情况下, 确定所述验证不通过。

20 16. 根据权利要求 15 所述的方法, 还包括:

在所述第一图片与所述第三图片一致的情况下, 确定所述验证通过; 以及

将所述业务数据发送给所述第二用户的终端。

17. 一种验证二维码的方法, 包括:

从第二用户的终端接收二维码信息和第一图片;

25 基于所述二维码信息, 获取二维码的内容数据;

基于所述二维码的内容数据, 获取业务数据和第二图片信息;

基于所述第一图片与所述第二图片信息, 确定所述第一图片与所述第二图片的相似
度; 以及

在所述相似度低于预定阈值时, 确定所述验证不通过。

30 18. 根据权利要求 17 所述的方法, 其中, 基于所述二维码的内容数据, 获取业务数据和第二图片信息包括, 通过预定解密方法对所述二维码的内容数据进行解密, 从而获

取业务数据和第二图片。

19. 根据权利要求 17 所述的方法，其中，从第二用户的终端接收二维码信息和第一图片包括，从第二用户的终端接收业务码，其中，所述业务码中包括叠加的二维码和所述第一图片。

5 20. 根据权利要求 17 所述的方法，其中，所述二维码信息包括二维码的内容数据。

21. 根据权利要求 17 所述的方法，其中，所述业务数据包括第三用户的用户标识，所述方法还包括：

在所述第一图片与所述第二图片相似度高于预定阈值的情况下，基于预存的用户标识与图片的关联关系，获取与所述第三用户的用户标识对应的第三图片；

10 确定所述第一图片与所述第三图片是否一致；以及

在所述第一图片与所述第三图片不一致的情况下，确定所述验证不通过。

22. 根据权利要求 21 所述的方法，还包括：

在所述第一图片与所述第三图片一致的情况下，确定所述验证通过；以及
将所述业务数据发送给所述第二用户的终端。

15 23. 一种提供二维码的装置，包括：

接收单元，配置为，从第一用户的终端接收二维码生成请求，所述请求中包括该二维码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；

获取单元，配置为，获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

20 存储单元，配置为，存储所述用户标识与所述第一图片的关联关系；

生成单元，配置为，基于所述业务数据生成二维码；以及

提供单元，配置为，将所述二维码和所述第一图片提供给所述第一用户。

24. 一种提供二维码的装置，包括：

接收单元，配置为，从第一用户的终端接收二维码生成请求，所述请求中包括该二

25 维码对应的业务数据，其中，所述业务数据包括所述第一用户的用户标识；

获取单元，配置为，获取第一图片以与所述用户标识相对应，其中，所述第一图片为肉眼可识别图片；

存储单元，配置为，存储所述用户标识与所述第一图片的关联关系；

生成单元，配置为，基于所述第一图片与所述业务数据生成二维码；以及

30 提供单元，配置为，将所述二维码和所述第一图片提供给所述第一用户。

25. 根据权利要求 23 或 24 所述的装置，其中所述提供单元还包括，叠加子单元，

配置为,通过叠加所述第一图片和所述二维码获取业务码,以及,提供子单元,配置为,将所述业务码提供给所述第一用户。

26. 根据权利要求 25 所述的装置,其中所述第一图片为二维码识别设备能够读取的图片。

5 27. 根据权利要求 25 所述的装置,其中,所述第一图片位于所述二维码内部。

28. 根据权利要求 27 所述的装置,其中,所述第一图片的面积基于所述二维码的纠错级别确定。

29. 根据权利要求 23 或 24 所述的装置,其中,所述第一图片包括以下至少一种内容:图案、文字、数字、符号。

10 30. 根据权利要求 23 或 24 所述的装置,其中,所述第一图片的用于对应于其他用户标识的重复获取率低于第一预定值。

31. 根据权利要求 30 所述的装置,其中,所述用户标识与所述第一图片唯一对应。

32. 根据权利要求 30 所述的装置,其中,所述获取单元还配置为,从预先建立的图库中获取与所述用户标识对应的第一图片,其中,所述图库包括数量多于预定值的图片。

15 33. 根据权利要求 32 所述的装置,还包括标记单元,配置为,在从预先建立的图库中获取与所述用户标识对应的第一图片之后,在所述图库中对所述第一图片进行标记。

34. 根据权利要求 32 或 33 所述的装置,其中,所述获取单元还配置为,从预先建立的图库中随机获取与所述用户标识对应的第一图片。

20 35. 根据权利要求 24 所述的装置,其中,所述第一图片的图像数据量小于等于第二预定值。

36. 根据权利要求 24 所述的装置,其中,所述生成单元包括,加密子单元,配置为,通过预定加密方法对所述第一图片与所述业务数据的组合进行加密以获取加密数据,以及生成子单元,配置为,基于所述加密数据生成二维码。

37. 一种验证二维码的装置,包括:

25 接收单元,配置为,从第二用户的终端接收二维码信息和第一图片;

第一获取单元,配置为,基于所述二维码信息,获取二维码的内容数据;

第二获取单元,配置为,基于所述二维码的内容数据,获取业务数据,其中,所述业务数据中包括第三用户的用户标识;

30 第三获取单元,配置为,基于预存的用户标识与图片的关联关系,获取与所述第三用户的用户标识对应的第三图片;

第一确定单元,配置为,确定所述第一图片与所述第三图片是否一致;以及

第二确定单元,配置为,在所述第一图片与所述第三图片不一致的情况下,确定所述验证不通过。

38. 根据权利要求 37 所述的装置,还包括:

第三确定单元,配置为,在所述第一图片与所述第三图片一致的情况下,确定所述

5 验证通过;以及

发送单元,配置为,将所述业务数据发送给所述第二用户的终端。

39. 一种验证二维码的装置,包括:

接收单元,配置为,从第二用户的终端接收二维码信息和第一图片;

第一获取单元,配置为,基于所述二维码信息,获取二维码的内容数据;

10 第二获取单元,配置为,基于所述二维码的内容数据,获取业务数据和第二图片信息;

第一确定单元,配置为,基于所述第一图片和所述第二图片信息,确定所述第一图片与所述第二图片的相似度;以及

第二确定单元,配置为,在所述相似度低于预定阈值时,确定所述验证不通过。

15 40. 根据权利要求 39 所述的装置,其中,所述第二获取单元还配置为,通过预定解密方法对所述二维码的内容数据进行解密,从而获取业务数据和第二图片。

41. 根据权利要求 39 所述的装置,其中,所述接收单元还配置为,从第二用户的终端接收业务码,其中,所述业务码中包括叠加的二维码和所述第一图片。

42. 根据权利要求 39 所述的装置,其中,所述二维码信息包括二维码的内容数据。

20 43. 根据权利要求 39 所述的装置,其中,所述业务数据包括第三用户的用户标识,所述装置还包括:

第三获取单元,配置为,在所述第一图片与所述第二图片相似度高于预定阈值的情况下,基于预存的用户标识与图片的关联关系,获取与所述第三用户的用户标识对应的第三图片;

25 第三确定单元,配置为,确定所述第一图片与所述第三图片是否一致;以及

第四确定单元,配置为,在所述第一图片与所述第三图片不一致的情况下,确定所述验证不通过。

44. 根据权利要求 43 所述的装置,还包括:

第五确定单元,配置为,在所述第一图片与所述第三图片一致的情况下,确定所述

30 验证通过;以及

发送单元,配置为,将所述业务数据发送给所述第二用户的终端。

45. 一种计算设备，包括存储器和处理器，其特征在于，所述存储器中存储有可执行代码，所述处理器执行所述可执行代码时，实现权利要求 1-22 中任一项所述的方法。