(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 111539502 B
(45)授权公告日 2021.10.15

(21)申请号 202010204983.6
(22)申请日 2020.03.25
(65)同一申请的已公布的文献号
申请公布号 CN 111539502 A
(43)申请公布日 2020.08.14
(73)专利权人 中国平安财产保险股份有限公司
地址 518000 广东省深圳市福田区益田路5033号平安金融中心12、13、38、39、40层
(72)发明人 黄嘉雯
(74)专利代理机构 深圳市力道知识产权代理事务所(普通合伙) 44507
代理人 何姣
(51)Int.Cl.
G06K 19/06(2006.01)
G06F 40/126(2020.01)
G06Q 30/00(2012.01)

审查员 栾越

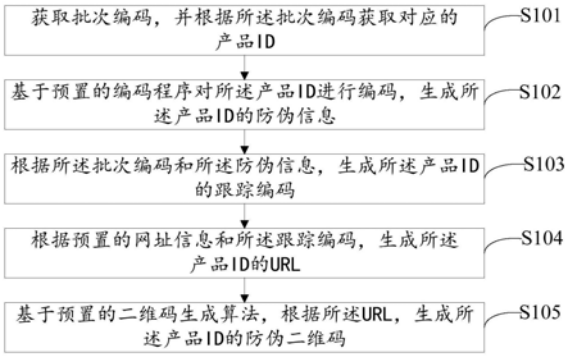
权利要求书2页 说明书12页 附图6页

(54)发明名称

防伪二维码的生成方法、装置、服务器及存储介质

(57)摘要

本发明涉及数据安全领域，提供了防伪二维码的生成方法、装置、服务器及计算机可读存储介质，包括：获取批次编码，并根据所述批次编码获取对应的产品ID；基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息；根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码；根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL；基于预置的二维码生成算法，根据所述URL，生成所述产品的防伪二维码，将产品ID的防伪信息生成URL，并将生成的URL作为二维码的生成信息，从而达到防伪的效果。



CN 111539502 B

1.一种防伪二维码的生成方法,其特征在于,包括:

获取批次编码,并根据所述批次编码获取对应的产品ID,所述产品ID为多个;

基于预置的编码程序对所述产品ID进行编码,生成所述产品ID的防伪信息;

将所述防伪信息和所述批次编码进行组合,生成所述产品ID的跟踪编码;

根据预置的网址信息和所述跟踪编码,生成所述产品ID的URL;

基于预置的二维码生成算法,根据所述URL,生成所述产品ID的防伪二维码;

其中,所述将所述防伪信息和所述批次编码进行组合,生成所述产品ID的跟踪编码,包括:

将所述防伪信息的防伪符号或防伪数字与所述批次编码的生产年份、生产月份和批生产次数进行组合,生成所述产品ID的跟踪编码。

2.如权利要求1所述的防伪二维码的生成方法,其特征在于,所述基于预置的编码程序对所述产品ID进行编码,生成所述产品ID的防伪信息包括:

基于所述编码程序将所述产品ID和预置编码进行组合,生成所述产品ID对应的防伪编码;

获取所述防伪编码的生成时间戳,将所述产品ID、防伪编码以及所述生成时间戳作为防伪信息。

3.如权利要求2所述的防伪二维码的生成方法,其特征在于,所述将所述防伪信息和所述批次编码进行组合,生成所述产品ID的跟踪编码包括:

基于预置的哈希算法程序,依次对所述批次编码、产品ID、防伪编码以及生成时间戳计算,分别得到所述批次编码、产品ID、防伪编码以及生成时间戳的哈希值;

将得到的所述批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合,生成所述产品ID的跟踪编码。

4.如权利要求3所述的防伪二维码的生成方法,其特征在于,所述将得到的所述批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合,生成所述产品ID的跟踪编码包括:

将得到的所述产品的批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合后,映射为二进制字符串;

若所述二进制字符串的长度小于目标长度时,对所述二进制字符串进行补位,生成与所述目标长度相同的跟踪编码。

5.如权利要求1-4中任意一项所述的防伪二维码的生成方法,其特征在于,所述基于预置的二维码生成算法,根据所述URL,生成所述产品ID的防伪二维码包括:

基于预置的二维码生成算法,确定所述URL的字符类型,并按所述字符类型对应的字符集将所述URL转换为数据字符串;

对所述数据字符串进行数据编码,得到所述数据字符串对应的第一码字序列;

通过预置纠错编码等级,对所述第一码字序列进行纠错编码,获取所述第一码字序列的纠错码字;

将所述纠错码字加入到所述第一码字序列后,以生成第二码字序列,并将所述第二码字序列添加至预置矩阵中,以生成所述产品ID的防伪二维码。

6.如权利要求5所述的防伪二维码的生成方法,其特征在于,所述将所述第二码字序列

添加至预置矩阵中，以生成所述产品ID的防伪二维码之后，包括：

接收终端扫描所述二维码触发的访问请求，获取所述访问请求携带的跟踪编码；

基于所述跟踪编码，查询所述跟踪编码对应的预置防伪信息，并对所述跟踪编码进行解码，以获取所述跟踪编码中的防伪信息；

当所述防伪信息与预置防伪信息不一致时，向所述终端发送异常提示信息。

7.如权利要求6所述的防伪二维码的生成方法，其特征在于，所述对所述跟踪编码进行解码，以获取所述跟踪编码中的防伪信息之后，还包括：

当所述防伪信息与所述预置防伪信息一致时，获取所述访问请求携带的所述终端的目标ID信息和目标位置信息；

读取预置记录库中的ID信息和位置信息，将读取到所述ID信息和所述位置信息与所述目标ID信息和所述目标位置信息进行对比；

当所述ID信息与所述目标ID信息不一致，且所述位置信息与所述目标位置信息不一致时，向所述终端发送异常提示信息。

8.一种防伪二维码的生成装置，其特征在于，所述防伪二维码的生成装置包括：

获取模块，用于获取批次编码，并根据所述批次编码获取对应的产品ID，所述产品ID为多个；

防伪信息生成模块，用于基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息；

跟踪编码生成模块，用于将所述防伪信息的防伪符号或防伪数字与所述批次编码的生产年份、生产月份和批生产次数进行组合，生成所述产品ID的跟踪编码；

URL生成模块，用于根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL；

二维码生成模块，用于基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码。

9.一种服务器，其特征在于，所述服务器包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如权利要求1至7中任一项所述防伪二维码的生成方法的步骤。

10.一种计算机可读存储介质，其特征在于，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如权利要求1至7中任一项所述的防伪二维码的生成方法的步骤。

防伪二维码的生成方法、装置、服务器及存储介质

技术领域

[0001] 本发明涉及数据安全技术领域，尤其涉及防伪二维码的生成方法、装置、服务器及计算机可读存储介质。

背景技术

[0002] 二维码(2-dimensional bar code)，又称二维条码，最早起源于日本，它是用特定的几何图形按一定规律在平面(二维方向)上分布的黑白相间的图形，是所有信息数据的一把钥匙。

[0003] 目前市面上产品溯源类身份标识码一般是使用二维码，通过将产品的企业信息或产品的属性信息，如生产信息、产品名称、产品用途等信息记录在管理平台上，用户通过扫描产品上的二维码来获取该产品在管理平台上记录的企业信息或产品的属性信息，虽能作为该产品回溯的窗口，但只是产品信息的展示，不能达到防伪的效果。

发明内容

[0004] 本发明的主要目的在于提供一种防伪二维码的生成方法、装置、服务器及计算机可读存储介质，旨在解决现有的二维码虽能作为该产品回溯的窗口，但只是产品信息的展示，不能达到防伪效果的技术问题。

[0005] 第一方面，本申请一种防伪二维码的生成方法，包括：

[0006] 获取批次编码，并根据所述批次编码获取对应的产品ID；

[0007] 基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息；

[0008] 根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码；

[0009] 根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL；

[0010] 基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码。

[0011] 第二方面，本申请还提供一种防伪二维码的生成装置，防伪二维码的生成装置包括：

[0012] 获取模块，用于获取批次编码，并根据所述批次编码获取对应的产品ID；

[0013] 防伪信息生成模块，用于基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息；

[0014] 跟踪编码生成模块，用于根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码；

[0015] URL生成模块，用于根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL；

[0016] 二维码生成模块，用于基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码。

[0017] 第三方面，本申请还提供一种服务器，所述服务器包括：存储器、处理器及存储在所述存储器上并可在所述处理器上运行的计算机程序，所述计算机程序被所述处理器执行时实现如上发明所述防伪二维码的生成方法的步骤。

[0018] 第四方面，本申请还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序被处理器执行时实现如上发明所述的防伪二维码的生成方法的步骤。

[0019] 本发明实施例提出的一种防伪二维码的生成方法、装置、服务器及计算机可读存储介质，获取批次编码，并根据所述批次编码获取对应的产品ID；基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息；根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码；根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL；基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码，实现了通过将产品的防伪信息生成URL，并将生成的URL作为二维码的生成信息，从而达到防伪的效果。

附图说明

[0020] 为了更清楚地说明本申请实施例技术方案，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，下面描述中的附图是本申请的一些实施例，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。

[0021] 图1为本申请实施例提供的一种防伪二维码的生成方法的流程示意图；

[0022] 图2为图1中的防伪二维码的生成方法的子步骤流程示意图；

[0023] 图3为图1中的防伪二维码的生成方法的子步骤流程示意图；

[0024] 图4为图1中的防伪二维码的生成方法的子步骤流程示意图；

[0025] 图5为本申请实施例提供的另一种防伪二维码的生成方法的流程示意图；

[0026] 图6为本申请实施例提供的一种防伪二维码的生成装置的示意性框图；

[0027] 图7为本申请实施例提供的另一种防伪二维码的生成装置的示意性框图；

[0028] 图8为本申请一实施例涉及的计算机设备的结构示意框图。

[0029] 本申请目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

[0030] 下面将结合本申请实施例中的附图，对本申请实施例中的技术方案进行清楚、完整地描述，显然，所描述的实施例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。

[0031] 附图中所示的流程图仅是示例说明，不是必须包括所有的内容和操作/步骤，也不是必须按所描述的顺序执行。例如，有的操作/步骤还可以分解、组合或部分合并，因此实际执行的顺序有可能根据实际情况改变。

[0032] 本申请实施例提供一种防伪二维码的生成方法、装置、服务器及计算机可读存储介质。其中，该防伪二维码的生成方法可应用于服务器中。

[0033] 下面结合附图，对本申请的一些实施方式作详细说明。在不冲突的情况下，下述的实施例及实施例中的特征可以相互组合。

[0034] 请参照图1，图1为本申请的实施例提供的一种防伪二维码的生成方法的流程示意图。

[0035] 如图1所示，该防伪二维码的生成方法包括步骤S101至步骤S105。

[0036] 步骤S101、获取产品的批次编码，并根据所述批次编码获取对应的产品ID；

[0037] 当服务器在读取到产品的批次编码，批次编码是产品的生产批次号，用于识别“批”的一组数字或字母加数字，例如，生产年份+生产月份+批生产次数，一般由生产时间的年、月、日各二位数组成。调用预置的编码程序或编码器，通过预置的编码程序或编码器将产品的批次编码进行编码，生成产品的应用程序。编码是信息从一种形式或格式转换为另一种形式的过程也称为计算机编程语言的代码简称编码。用预先规定的编码规则将文字、数字或其它对象编成数码信息，或将信息、数据转换成规定的电脉冲信号。例如，服务器在获取到批次编码的生产年份+生产月份+批生产次数时，通过预置的编码程序或编码器将生产年份+生产月份+批生产次数编码为图形、文字等形式的数码信息。

[0038] 示范例为，服务器获取产品的批次编码，通过该批次编码获取与产品ID之间的映射关系表。预先将产品的批次编码与产品ID之间的信息设置为映射关系表，例如，在映射关系表中记录批次编码，以及该批次编码的所有产品ID号，且每一个产品都有一个产品ID，各个产品ID不相同。一个产品批次包括不止一个产品ID，将所有的产品ID与产品的批次编码进行关联，生成映射关系表。通过该映射关系表，获取该批次编码对应的产品ID，该ID可以是数字、字母或特殊字符等组合，且获取到的产品ID不至一个，对此对获取到的产品ID数量不做限定。

[0039] 步骤S102、基于预置的编码程序对所述产品ID进行编码，生成所述产品的防伪信息；

[0040] 在获取到产品ID时，调取预置的编码程序。编码程序中的编码是信息从一种形式或格式转换为另一种形式的过程也称为计算机编程语言的代码简称编码。用预先规定的编码规则将文字、数字或其它对象编成数码信息，或将信息、数据转换成规定的电脉冲信号。通过编码程序对产品ID进行编码，生成该产品的防伪信息。

[0041] 在一实施例中，具体地，参照图2，步骤S102包括：子步骤S1021至子步骤S1022。

[0042] 子步骤S1021、基于所述编码程序将所述产品ID和预置编码进行组合，生成所述产品ID对应的防伪编码；

[0043] 获取编码程序中的预置编码，通过编码程序将产品ID和预置编码进行组合，生成产品对应的防伪编码。组合的方式有两种，实施例为，固定组合，将预置编码放在前面，将产品ID放在预置编码后面。例如，预置编码为1234为，产品ID为00012时，防伪编码为123400012。或者，产品ID前面，置编码放在产品ID后面，防伪编码为000121234。随机组合，将预置编码和产品ID打乱，重新进行组合。例如，预置编码为1234为，产品ID为00012时，防伪编码为010423021等。

[0044] 子步骤S1022、获取所述防伪编码的生成时间戳，将所述产品ID、防伪编码以及所述生成时间戳作为防伪信息。

[0045] 当生成防伪编码时，获取生成防伪编码的生成时间。例如，当检测到成功生成防伪编码，记录当前时间系统的时刻，将记录的时刻作为生成时间戳。将产品ID、防伪编码以及生成时间戳作为防伪信息，每一个产品ID都有一个防伪信息，且各个产品ID的防伪信息不相同。

[0046] 步骤S103、根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码；

[0047] 在获取到防伪信息时，将获取到的防伪信息和批次编码进行组合，生成该产品的

跟踪编码。例如，当防伪信息为一个防伪符号、一组防伪数字等，批次编码为产品的生产年份+生产月份+批生产次数，将防伪信息的防伪符号或防伪数字与产品的生产年份+生产月份+批生产次数进行组合，组合的顺序不做规定，生成产品ID的跟踪编码。

[0048] 在一实施例中，具体地，参照图3，步骤S103包括：子步骤S1031至子步骤S1032。

[0049] 子步骤S1031，基于预置的哈希算法程序，依次对批次编码、产品ID、防伪编码以及生成时间戳计算，分别得到批次编码、产品ID、防伪编码以及生成时间戳的哈希值；

[0050] 当服务器在获取到产品的跟踪编码时，调取预置的哈希算法程序。哈希算法程序将任意长度的二进制值映射为较短的固定长度的二进制值，这个小的二进制值称为哈希值。哈希值是一段数据唯一且极其紧凑的数值表示形式。如果散列一段明文而且哪怕只更改该段落的一个字母，随后的哈希都将产生不同的值。要找到散列为同一个值的两个不同的输入，数据的哈希值可以检验数据的完整性。通过预置的哈希算法分别对对批次编码、产品ID、防伪编码以及生成时间戳计算，得到批次编码、产品ID、防伪编码以及生成时间戳的哈希值。例如，通过预置的哈希算法程序对批次编码进行计算，得到批次编码的哈希值，再对产品ID进行计算，得到产品ID的哈希值，再对防伪编码进行计算，得到防伪编码的哈希值，再对生成时间戳进行计算，得到生成时间戳的哈希值。

[0051] 子步骤S1032，将得到的批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合，生成产品ID的跟踪编码。

[0052] 当服务器分别得到批次编码的哈希值、产品ID的哈希值、防伪编码的哈希值以及生成时间戳的哈希值时，将得到的批次编码的哈希值、产品ID的哈希值、防伪编码的哈希值以及生成时间戳的哈希值进行组合，生成产品的跟踪编码。例如，组合方式可以是批次编码的哈希值+产品ID的哈希值+防伪编码的哈希值+生成时间戳的哈希值的组合方式，生成产品的跟踪编码，也可以是产品ID的哈希值+生成时间戳的哈希值+防伪编码的哈希值+批次编码的哈希值的方式，生成产品ID的跟踪编码，对此组合的方式不做限定。

[0053] 还包括服务器将得到的产品的批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合后，映射为二进制字符串；若二进制字符串的长度小于目标长度时，对二进制字符串进行补位，生成与目标长度相同的跟踪编码。例如，在得到产品的批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合后映射的二进制字符串，获取该二进制字符串的长度，将获取到的长度与预置的目标长度进行对比，将该二进制字符串的长度小于目标长度时，对该二进制字符串的长度进行补位，例如，二进制字符串的长度为16为时，目标长度为18位时，在二进制字符串补两个0，以使二进制字符串的长度与目标长度相同，生成与目标长度相同的跟踪编码。

[0054] 步骤S104、根据预置的网址信息和跟踪编码，生成产品ID的URL；

[0055] 当终端在获取到产品的跟踪编码时，读取预置网址信息。网址信息预先存储在预置路径中，例如，将http://ecos-agrpingan.com.cn存储在预置路径中，终端通过读取到的预置网址信息和产品的跟踪编码，将预置网址信息和处理产品的跟踪编码进行组合，生成产品的URL，URL是统一资源定位符(Uniform Resource Locator，URL)是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。

[0056] 步骤S105、基于预置的二维码生成算法，根据URL，生成产品ID的防伪二维码。

[0057] 服务器在获取到产品的URL时，通过预置的二维码生成算法对该产品的URL进行编

码,生成产品的二维码。二维码生成算法可以是Data Matrix,Maxi Code,Aztec,QR Code等,且二维码包括堆叠式二维码和矩阵式二维码,其中堆叠式二维码是建立在一维条码基础之上,按需要堆积成二行或多行。它在编码设计、校验原理、识读方式等方面继承了一维条码的一些特点,识读设备与条码印刷与一维条码技术兼容。但由于行数的增加,需要对行进行判定,其译码算法与软件也不完全相同于一维条码。行排式二维条码有:Code16K、Code49、PDF417、MicroPDF417等。矩阵式二维条码(又称棋盘式二维条码)它是在一个矩形空间通过黑、白像素在矩阵中的不同分布进行编码。在矩阵相应元素位置上,用点(方点、圆点或其他形状)的出现表示二进制“1”,点的不出现表示二进制的“0”,点的排列组合确定了矩阵式二维条码所代表的意义。矩阵式二维条码是建立在计算机图像处理技术、组合编码原理等基础上的一种新型图形符号自动识读处理码制。具有代表性的矩阵式二维条码有:Code One、MaxiCode、QR Code等。

[0058] 在一实施例中,具体地,参照图4,步骤S105包括:子步骤S1051至子步骤S1054。

[0059] 子步骤S1051、基于预置的二维码生成算法,确定URL的字符类型,并按字符类型对应的字符集将URL转换为数据字符串;

[0060] 服务器通过预置的二维码生成算法,对URL进行数据分析,确定URL的字符类型,按相应的字符集将URL转换成数据字符串。其中,预置的二维码生成算法为QB二维码生成算法。例如,对URL进行数据分析,确定URL的字符类型,当确定URL为数字时,选择数字对应的字符集,当URL为英文时,选择英文对应的字符集,通过字符集中对应的数据字符,分别将URL转换为数据字符,再讲数据字符进行组合,生成URL的数据字符串。

[0061] 子步骤S1052、对所述数据字符串进行数据编码,得到所述数据字符串对应的第一码字序列;

[0062] 通过对URL的数据字符串进行数据编码,将数据字符串转换为位流,每8位一个码字,整体构成一个数据的码字序列。数据可以按照一种模式进行编码,以便进行更高效的解码,例如:对数据:01234567编码,分组:012 34567,转成二进制:012→0000001100、345→0101011001、67→1000011、转成序列:0000001100 0101011001 1000011、字符数转成二进制:8→0000001000、加入模式指示符(上图数字)0001:0001 0000001000 0000001100 0101011001 1000011,以此得到该数据字符串的第一码字序列。

[0063] 子步骤S1053、通过预置纠错编码等级,对第一码字序列进行纠错编码,获取第一码字序列的纠错码字;

[0064] 选择URL的纠错等级,在预置规则条件下,纠错等级越高其真实数据的容量越小。通过URL的纠错等级对URL的数据字符串进行纠错编码,按需要将上面的码字序列分块,并根据纠错等级和分块的码字,获取纠错码字。在二维码规格和纠错等级确定的情况下,其实它所能容纳的码字总数和纠错码字数也就确定了,比如:版本10,纠错等级时H时,总共能容纳346个码字,其中224个纠错码字,就是说二维码区域中大约1/3的码字时冗余的。对于这224个纠错码字,它能够纠正112个替代错误(如黑白颠倒)或者224个据读错误(无法读到或者无法译码)。

[0065] 子步骤S1054、将所述纠错码字加入到第一码字序列后,以生成第二码字序列,并将所述第二码字序列添加至预置矩阵中,以生成所述产品ID的防伪二维码。

[0066] 在获取待该纠错码字时,将该纠错码字放入第一码字序列后,以生成第二码字序

列。通过预置的矩阵构造最终数据信息，在矩阵规格确定的条件下，将上面产生的序列按次序放如分块中。例如，按规定把数据分块，然后对每一块进行计算，得出相应的纠错码字区块，把纠错码字区块按顺序构成一个序列，添加到原先的数据。如：D1,D12,D23,D35,D2,D13,D24,D36,...D11,D22,D33,D45,D34,D46,E1,E23,E45,E67,E2,E24,E46,E68,...。将探测图形、分隔符、定位图形、校正图形和码字模块放入矩阵中，把上面的完整序列填充到相应矩阵规格的二维码矩阵的区域中，生成防伪二维码。

[0067] 在本实施例中，通过将产品ID生成防伪信息，将该防伪信息生成URL，并将生成的URL作为二维码的生成信息，使二维码中包含有产品的防伪信息达到防伪的效果。

[0068] 请参照图5，图5为实施本实施例提供的防伪溯源二维码的生成方法的流程示意图。

[0069] 如图5所示，该防伪溯源二维码的生成方法包括步骤S201至S211。

[0070] 步骤S201、获取产品的批次编码，并根据所述批次编码获取对应的产品ID。

[0071] 当服务器在读取到产品的批次编码，批次编码是产品的生产批次号，用于识别“批”的一组数字或字母加数字，例如，生产年份+生产月份+批生产次数，一般由生产时间的年、月、日各二位数组成。调用预置的编码程序或编码器，通过预置的编码程序或编码器将产品的批次编码进行编码，生成产品的应用程序。编码是信息从一种形式或格式转换为另一种形式的过程也称为计算机编程语言的代码简称编码。用预先规定的编码规则将文字、数字或其它对象编成数码信息，或将信息、数据转换成规定的电脉冲信号。例如，服务器在获取到批次编码的生产年份+生产月份+批生产次数时，通过预置的编码程序或编码器将生产年份+生产月份+批生产次数编码为图形、文字等形式的数码信息。

[0072] 示范例为，服务器获取产品的批次编码，通过该批次编码获取与产品ID之间的映射关系表。预先将产品的批次编码与产品ID之间的信息设置为映射关系表，例如，在映射关系表中记录批次编码，以及该批次编码的所有产品ID号，且每一个产品都有一个产品ID，各个产品ID不相同。一个产品批次包括不止一个产品ID，将所有的产品ID与产品的批次编码进行关联，生成映射关系表。通过该映射关系表，获取该批次编码对应的产品ID，该ID可以是数字、字母或特殊字符等组合，且获取到的产品ID不至一个，对此对获取到的产品ID数量不做限定。

[0073] 步骤S202、基于预置的编码程序对所述产品ID进行编码，生成所述产品的防伪信息。

[0074] 在获取到产品ID时，调取预置的编码程序。编码程序中的编码是信息从一种形式或格式转换为另一种形式的过程也称为计算机编程语言的代码简称编码。用预先规定的编码规则将文字、数字或其它对象编成数码信息，或将信息、数据转换成规定的电脉冲信号。通过编码程序对产品ID进行编码，生成该产品的防伪信息。

[0075] 步骤S203、根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码。

[0076] 在获取到防伪信息时，将获取到的防伪信息和批次编码进行组合，生成该产品的跟踪编码。例如，当防伪信息为一个防伪符号、一组防伪数字等，批次编码为产品的生产年份+生产月份+批生产次数，将防伪信息的防伪符号或防伪数字与产品的生产年份+生产月份+批生产次数进行组合，组合的顺序不做规定，生成产品的跟踪编码。

[0077] 步骤S204、根据预置的网址信息和所跟踪编码，生成产品ID的URL。

[0078] 当终端在获取到产品的跟踪编码时，读取预置网址信息。网址信息预先存储在预置路径中，例如，将http://ecos-agrpingan.com.cn存储在预置路径中，终端通过读取到的预置网址信息和产品的跟踪编码，将预置网址信息和处理产品的跟踪编码进行组合，生成产品的URL，URL是统一资源定位符(Uniform Resource Locator，URL)是对可以从互联网上得到的资源的位置和访问方法的一种简洁的表示，是互联网上标准资源的地址。

[0079] 步骤S205、基于预置的二维码生成算法，根据URL，生成产品ID的防伪二维码。

[0080] 服务器通过预置的二维码生成算法，对URL进行数据分析，确定URL的字符类型，按相应的字符集将URL转换成数据字符串。其中，预置的二维码生成算法为QB二维码生成算法。例如，对URL进行数据分析，确定URL的字符类型，当确定URL为数字时，选择数字对应的字符集，当URL为英文时，选择英文对应的字符集，通过字符集中对应的数据字符，分别将URL转换为数据字符，再讲数据字符进行组合，生成URL的数据字符串。

[0081] 通过对URL的数据字符串进行数据编码，将数据字符串转换为位流，每8位一个码字，整体构成一个数据的码字序列。数据可以按照一种模式进行编码，以便进行更高效的解码，例如：对数据：01234567编码，分组：012 345 67，转成二进制：012→0000001100、345→0101011001、67→1000011、转成序列：0000001100 0101011001 1000011、字符数转成二进制：8→0000001000、加入模式指示符(上图数字)0001：0001 0000001000 0000001100 0101011001 1000011。得到该数据字符串的第一码字序列。

[0082] 选择URL的纠错等级，在预置规则条件下，纠错等级越高其真实数据的容量越小。通过URL的纠错等级对URL的数据字符串进行纠错编码，按需要将上面的码字序列分块，并根据纠错等级和分块的码字，获取纠错码字。在二维码规格和纠错等级确定的情况下，其实它所能容纳的码字总数和纠错码字数也就确定了，比如：版本10，纠错等级时H时，总共能容纳346个码字，其中224个纠错码字，就是说二维码区域中大约1/3的码字时冗余的。对于这224个纠错码字，它能够纠正112个替代错误(如黑白颠倒)或者224个据读错误(无法读到或者无法译码)。

[0083] 在获取待该纠错码字时，将该纠错码字放入第一码字序列后，以生成第二码字序列。通过预置的矩阵构造最终数据信息，在矩阵规格确定的条件下，将上面产生的序列按次序放如分块中。例如，按规定把数据分块，然后对每一块进行计算，得出相应的纠错码字区块，把纠错码字区块按顺序构成一个序列，添加到原先的数据。如：D1,D12,D23,D35,D2,D13,D24,D36,...D11,D22,D33,D45,D34,D46,E1,E23,E45,E67,E2,E24,E46,E68,....将探测图形、分隔符、定位图形、校正图形和码字模块放入矩阵中，把上面的完整序列填充到相应矩阵规格的二维码矩阵的区域中，生成防伪二维码。

[0084] 步骤S206、接收终端扫描二维码触发的访问请求，获取访问请求携带的跟踪编码。

[0085] 服务器接收到扫描终端通过扫描二维码触发访问请求，获取该访问请求携带的跟踪编码。例如，扫描终端扫描产品上的防伪二维码时，该防伪二维码是基于URL编码生成的，而URL中包括跟踪编码，应该获取到该跟踪编码。

[0086] 步骤S207、基于跟踪编码，查询跟踪编码对应的预置防伪信息，并对跟踪编码进行解码，以获取跟踪编码中的防伪信息。

[0087] 服务器获取到该跟踪编码时，通过将该跟踪编码作为搜索条件，搜索到服务器存储中记录的该跟踪编码对应的预置防伪信息，并对该跟踪编码进行解析，获取该跟踪编码

中的防伪信息。预先将每一产品的跟踪编码和防伪信息都预先存储值服务器中，每一个产品的跟踪编码和防伪信息都不一样，且一一对应。

[0088] 步骤S208、当防伪信息与预置防伪信息不一致时，向终端发送异常提示信息。

[0089] 当防伪信息和预置防伪信息不一致时，服务器向终端发送异常提示系信息提示该产品已经被使用。例如，防伪信息和预置防伪信息中包括产品ID、防伪编码和生成时间戳，当防伪信息中的产品ID与预置防伪信息中的产品ID不一致，获防伪信息中的防伪编码与预置防伪信息中的防伪编码不一致，或防伪信息中的生成时间戳与预置防伪信息中的生成时间戳不一致，发送异常提示信息。

[0090] 步骤S209、当防伪信息与预置防伪信息一致时，获取访问请求携带的终端的目标ID信息和目标位置信息。

[0091] 当获取到的防伪信息和预置防伪信息时，将防伪信息和预置防伪信息进行对比，当防伪信息和预置防伪信息一致时，获取该访问请求携带的终端的目标ID信息和位置信息。例如，防伪信息和预置防伪信息中包括产品ID、防伪编码和生成时间戳，当防伪信息中的产品ID与预置防伪信息中的产品ID一致，获防伪信息中的防伪编码与预置防伪信息中的防伪编码一致，或防伪信息中的生成时间戳与预置防伪信息中的生成时间戳一致，获取访问请求携带的终端的目标ID信息和目标位置信息。

[0092] 步骤S210、读取预置记录库中的ID信息和位置信息，将读取到ID信息和位置信息与目标ID信息和目标位置信息进行对比。

[0093] 服务器将首次扫描该二维码的终端或扫描终端的ID信息和位置信息记录在存储有该产品信息的公有链中。当服务器获取预置记录库中的终端ID信息和位置信息时，将获取到的终端ID信息和位置信息与目标ID信息和目标位置信息进行比对，当服务器中的终端ID信息和位置信息与目标ID信息和目标位置信息相同时，服务器发送公有链中记录的该产品的生产责任主体信息、产品和批次基础信息、产品生产、检测和加工环节与投入品信息、物流和销售渠道信息。

[0094] 步骤S211、当ID信息与目标ID信息不一致，且位置信息与目标位置信息不一致时，向终端发送异常提示信息。

[0095] 当ID信息与目标ID信息不一致时，且位置信息与目标位置信息不一致，服务器向终端发送异常提示系信息提示该产品已经被使用。当ID信息与目标ID信息一致，且位置信息与目标位置信息不一致时，服务器发送公有链中记录的该产品的生产责任主体信息、产品和批次基础信息、产品生产、检测和加工环节与投入品信息、物流和销售渠道信息。

[0096] 在本实施例中，通过将产品ID生成防伪信息，将该防伪信息生成URL，并将生成的URL作为二维码的生成信息，以生成产品ID的防伪二维码，通过扫二维码，获取二维码中防伪信息验证当前产品是否为异常产品。

[0097] 请参照图6，图6为本申请实施例提供的一种防伪二维码的生成装置的示意性框图。

[0098] 如图6所示，该防伪二维码的生成装置400，包括：获取模块401、防伪信息生成模块402、跟踪编码生成模块403、URL生成模块404、二维码生成模块405。

[0099] 获取模块401，用于获取产品的批次编码，并根据所述批次编码获取对应的产品ID；

[0100] 防伪信息生成模块402，用于基于预置的编码程序对所述产品ID进行编码，生成所述产品的防伪信息；

[0101] 跟踪编码生成模块403，用于根据批次编码和防伪信息，生成产品ID的跟踪编码；

[0102] URL生成模块404，用于根据预置的网址信息和跟踪编码，生成产品ID的URL；

[0103] 二维码生成模块405，用于基于预置的二维码生成算法，根据URL，生成产品ID的防伪二维码。

[0104] 在一个实施例中，如图7所示，该防伪二维码的生成装置500，包括：获取模块501、防伪信息生成模块502、跟踪编码生成模块503、URL生成模块504、二维码生成模块505、获取跟踪编码模块506、获取防伪信息模块507、第一发送模块508、获取终端信息模块509、对比模块510、第二发送模块511。

[0105] 获取模块501，用于获取产品的批次编码，并根据所述批次编码获取对应的产品ID；

[0106] 防伪信息生成模块502，用于基于预置的编码程序对所述产品ID进行编码，生成所述产品的防伪信息；

[0107] 跟踪编码生成模块503，用于根据批次编码和所述防伪信息，生成产品ID的跟踪编码；

[0108] URL生成模块504，用于根据预置的网址信息和跟踪编码，生成产品ID的URL；

[0109] 二维码生成模块505，用于基于预置的二维码生成算法，根据URL，生成产品ID的防伪二维码；

[0110] 获取跟踪编码模块506，用于接收终端扫描所述二维码触发的访问请求，获取所述访问请求携带的跟踪编码；

[0111] 获取防伪信息模块507，用于基于所述跟踪编码，查询所述跟踪编码对应的预置防伪信息，并对所述跟踪编码进行解码，以获取所述跟踪编码中的防伪信息；

[0112] 第一发送模块508，用于当所述防伪信息与预置防伪信息不一致时，向所述终端发送异常提示信息；

[0113] 获取终端信息模块509，用于当所述防伪信息与所述预置防伪信息一致时，获取所述访问请求携带的所述终端的目标ID信息和目标位置信息；

[0114] 对比模块510，用于读取预置记录库中的ID信息和位置信息，将读取到所述ID信息和所述位置信息与所述目标ID信息和所述目标位置信息进行对比；

[0115] 第二发送模块511，用于当所述ID信息与所述目标ID信息不一致，且所述位置信息与所述目标位置信息不一致时，向所述终端发送异常提示信息。

[0116] 需要说明的是，所属领域的技术人员可以清楚地了解到，为了描述的方便和简洁，上述描述的装置和各模块及单元的具体工作过程，可以参考前述复合语音识别方法实施例中的对应过程，在此不再赘述。

[0117] 上述实施例提供的装置可以实现为一种计算机程序的形式，该计算机程序可以在如图8所示的计算机设备上运行。

[0118] 请参阅图8，图8为本申请实施例提供的一种计算机设备的结构示意性框图。该计算机设备可以为终端。

[0119] 如图8所示，该计算机设备包括通过系统总线连接的处理器、存储器和网络接口，

其中,存储器可以包括非易失性存储介质和内存储器。

[0120] 非易失性存储介质可存储操作系统和计算机程序。该计算机程序包括程序指令,该程序指令被执行时,可使得处理器执行任意一种防伪二维码的生成方法。

[0121] 处理器用于提供计算和控制能力,支撑整个计算机设备的运行。

[0122] 内存储器为非易失性存储介质中的计算机程序的运行提供环境,该计算机程序被处理器执行时,可使得处理器执行任意一种防伪二维码的生成方法。

[0123] 该网络接口用于进行网络通信,如发送分配的任务等。本领域技术人员可以理解,图8中示出的结构,仅仅是与本申请方案相关的部分结构的框图,并不构成对本申请方案所应用于其上的计算机设备的限定,具体地计算机设备可以包括比图中所示更多或更少的部件,或者组合某些部件,或者具有不同的部件布置。

[0124] 应当理解的是,处理器可以是中央处理单元(Central Processing Unit,CPU),该处理器还可以是其他通用处理器、数字信号处理器(Digital Signal Processor,DSP)、专用集成电路(Application Specific Integrated Circuit,ASIC)、现场可编程门阵列(Field-Programmable Gate Array,FPGA)或者其他可编程逻辑器件、分立门或者晶体管逻辑器件、分立硬件组件等。其中,通用处理器可以是微处理器或者该处理器也可以是任何常规的处理器等。

[0125] 其中,在一个实施例中,所述处理器用于运行存储在存储器中的计算机程序,以实现如下步骤:

[0126] 获取产品的批次编码,并根据所述批次编码获取对应的产品ID;

[0127] 基于预置的编码程序对所述产品ID进行编码,生成所述产品的防伪信息;

[0128] 根据所述批次编码和所述防伪信息,生成所述产品的跟踪编码;

[0129] 根据预置的网址信息和所述跟踪编码,生成所述产品的URL;

[0130] 基于预置的二维码生成算法,根据所述URL,生成所述产品的防伪二维码。

[0131] 在一个实施例中,所述处理器在实现基于预置的编码程序对所述产品ID进行编码,生成所述产品的防伪信息时,用于实现:

[0132] 基于所述编码程序将所述产品ID和预置编码进行组合,生成所述产品ID对应的防伪编码;

[0133] 获取所述防伪编码的生成时间戳,将所述产品ID、防伪编码以及所述生成时间戳作为防伪信息。

[0134] 在一个实施例中,所述处理器在实现根据所述批次编码和所述防伪信息,生成所述产品ID的跟踪编码时,用于实现:

[0135] 基于预置的哈希算法程序,依次对批次编码、产品ID、防伪编码以及生成时间戳计算,分别得到批次编码、产品ID、防伪编码以及生成时间戳的哈希值;

[0136] 将得到的批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合,生成产品ID的跟踪编码。

[0137] 在一个实施例中,所述处理器在实现将得到的所述批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合,生成所述产品ID的跟踪编码时,用于实现:

[0138] 将得到的产品的批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合后,映射为二进制字符串;

[0139] 若所述二进制字符串的长度小于目标长度时，对二进制字符串进行补位，生成与目标长度相同的跟踪编码。

[0140] 在一个实施例中，所述处理器在实现基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码时，用于实现：

[0141] 基于预置的二维码生成算法，确定URL的字符类型，并按字符类型对应的字符集将URL转换为数据字符串；

[0142] 对数据字符串进行数据编码，得到数据字符串对应的第一码字序列；

[0143] 通过预置纠错编码等级，对第一码字序列进行纠错编码，获取第一码字序列的纠错码字；

[0144] 将纠错码字加入到所述第一码字序列后，以生成第二码字序列，并将第二码字序列添加至预置矩阵中，以生成产品ID的防伪二维码。

[0145] 在一个实施例中，所述处理器在实现将所述第二码字序列添加至预置矩阵中，以生成所述产品的防伪二维码之后时，用于实现：

[0146] 接收终端扫描所述二维码触发的访问请求，获取访问请求携带的跟踪编码；

[0147] 基于跟踪编码，查询跟踪编码对应的预置防伪信息，并对跟踪编码进行解码，以获取跟踪编码中的防伪信息；

[0148] 当防伪信息与预置防伪信息不一致时，向终端发送异常提示信息。

[0149] 在一个实施例中，所述处理器在实现对所述跟踪编码进行解码，以获取所述跟踪编码中的防伪信息之后时，用于实现：

[0150] 当防伪信息与预置防伪信息一致时，获取访问请求携带的终端的目标ID信息和目标位置信息；

[0151] 读取预置记录库中的ID信息和位置信息，将读取到ID信息和位置信息与目标ID信息和目标位置信息进行对比；

[0152] 当所述ID信息与目标ID信息不一致，且位置信息与目标位置信息不一致时，向终端发送异常提示信息。

[0153] 本申请实施例还提供一种计算机可读存储介质，所述计算机可读存储介质上存储有计算机程序，所述计算机程序中包括程序指令，所述程序指令被执行时所实现的方法可参照本申请防伪二维码的生成方法的各个实施例。

[0154] 其中，所述计算机可读存储介质可以是前述实施例所述的计算机设备的内部存储单元，例如所述计算机设备的硬盘或内存。所述计算机可读存储介质也可以是所述计算机设备的外部存储设备，例如所述计算机设备上配备的插接式硬盘，智能存储卡(Smart Media Card,SMC)，安全数字(Secure Digital,SD)卡，闪存卡(Flash Card)等。

[0155] 需要说明的是，在本文中，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、物品或者系统不仅包括那些要素，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、物品或者系统所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者系统中还存在另外的相同要素。

[0156] 上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

[0157] 通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方

法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在如上所述的一个存储介质(如ROM/RAM、磁碟、光盘)中，包括若干指令用以使得一台终端设备(可以是手机，计算机，服务器，空调器，或者网络设备等)执行本发明各个实施例所述的方法。

[0158] 以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

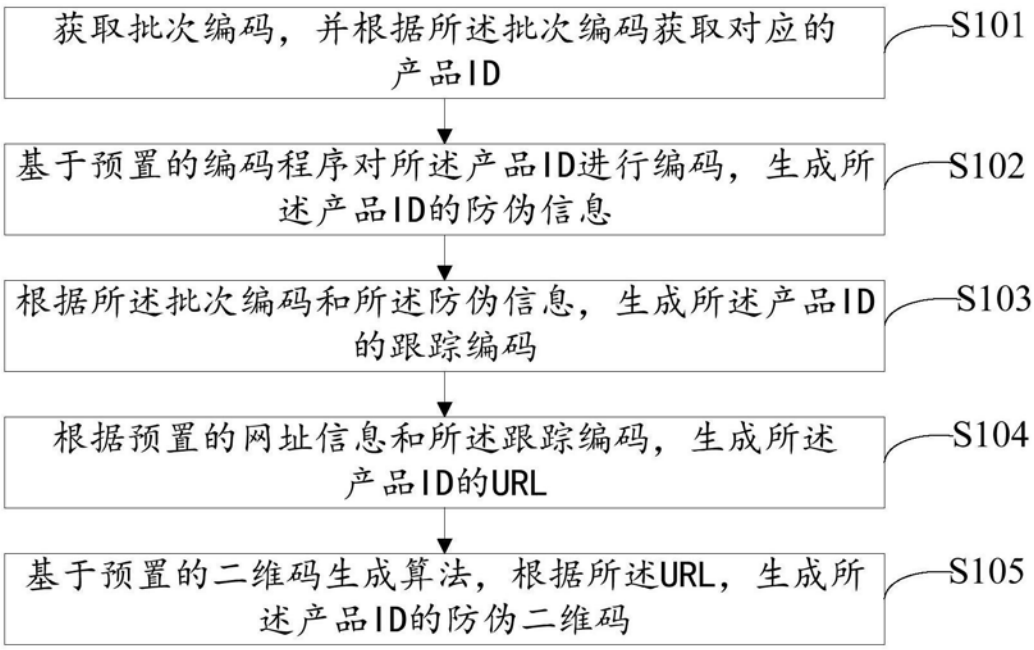

获取批次编码，并根据所述批次编码获取对应的产品ID
S101
基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息
S102
根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码
S103
根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL
S104
基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码
S105

图1

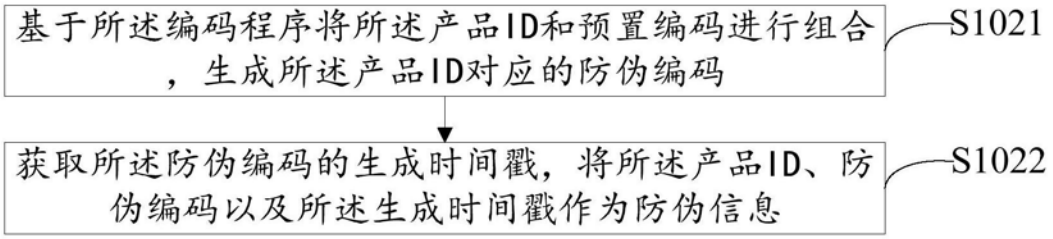

基于所述编码程序将所述产品ID和预置编码进行组合，生成所述产品ID对应的防伪编码
S1021
获取所述防伪编码的生成时间戳，将所述产品ID、防伪编码以及所述生成时间戳作为防伪信息
S1022

图2

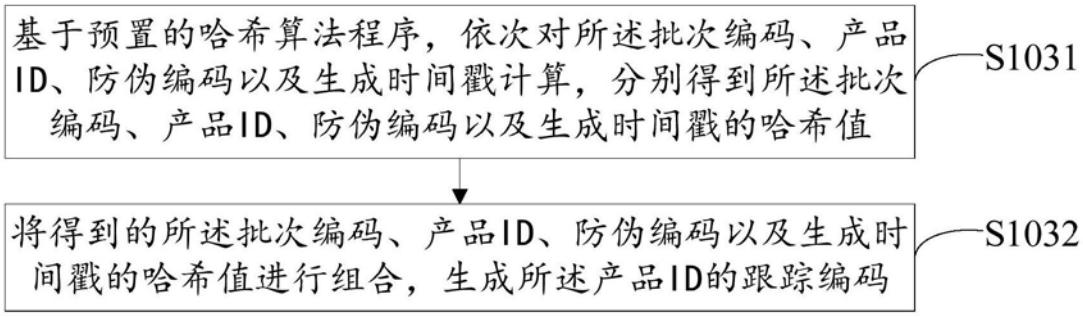

基于预置的哈希算法程序，依次对所述批次编码、产品ID、防伪编码以及生成时间戳计算，分别得到所述批次编码、产品ID、防伪编码以及生成时间戳的哈希值
S1031
将得到的所述批次编码、产品ID、防伪编码以及生成时间戳的哈希值进行组合，生成所述产品ID的跟踪编码
S1032

图3

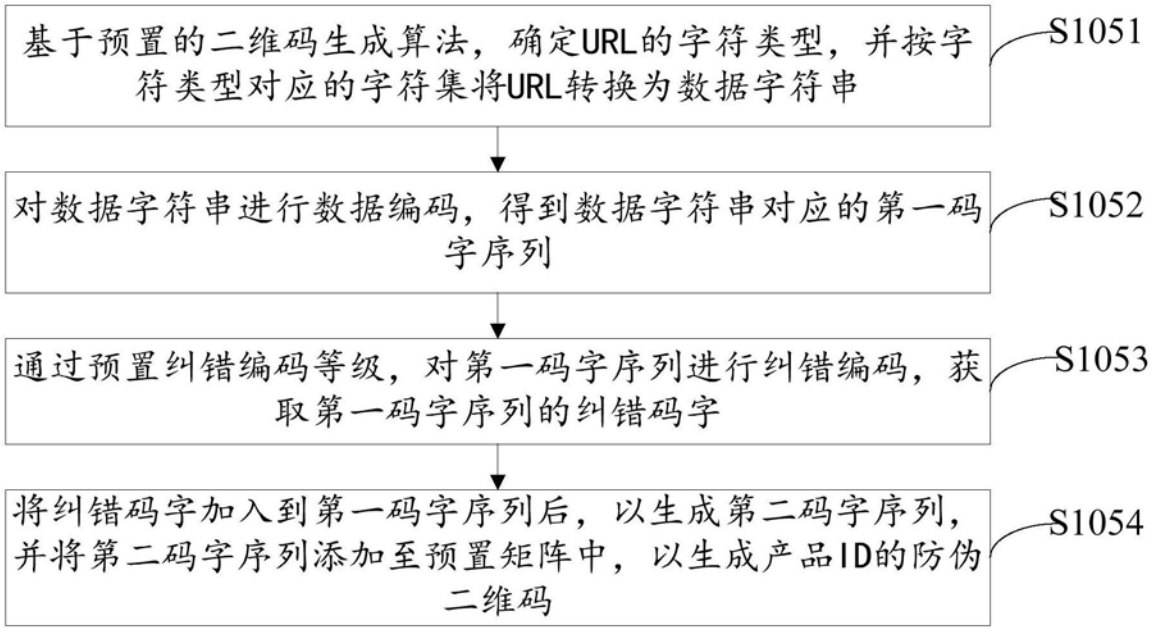

基于预置的二维码生成算法，确定URL的字符类型，并按字符类型对应的字符集将URL转换为数据字符串
S1051
对数据字符串进行数据编码，得到数据字符串对应的第一码字序列
S1052
通过预置纠错编码等级，对第一码字序列进行纠错编码，获取第一码字序列的纠错码字
S1053
将纠错码字加入到第一码字序列后，以生成第二码字序列，并将第二码字序列添加至预置矩阵中，以生成产品ID的防伪二维码
S1054

图4

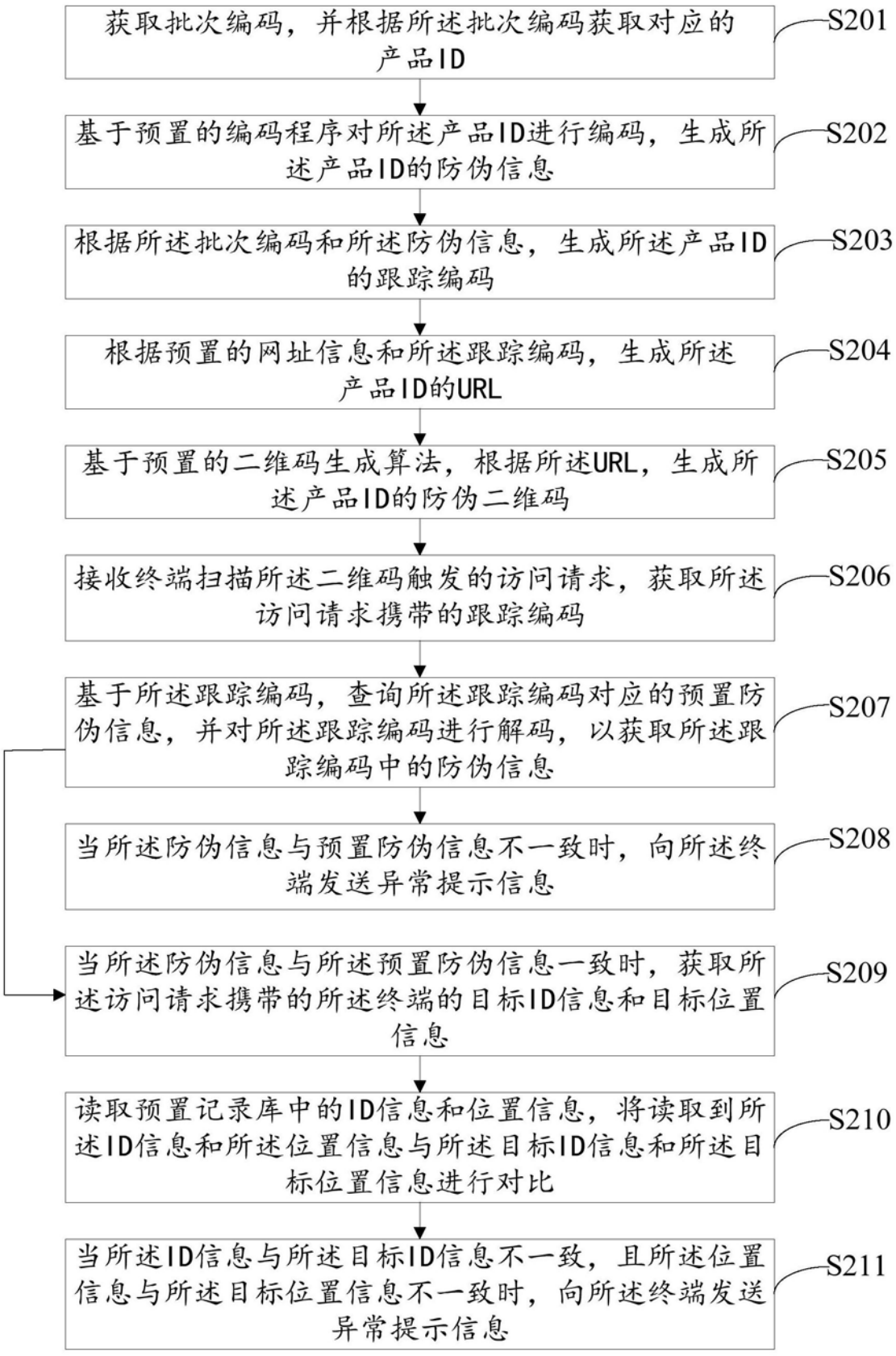

获取批次编码，并根据所述批次编码获取对应的产品ID
S201
基于预置的编码程序对所述产品ID进行编码，生成所述产品ID的防伪信息
S202
根据所述批次编码和所述防伪信息，生成所述产品ID的跟踪编码
S203
根据预置的网址信息和所述跟踪编码，生成所述产品ID的URL
S204
基于预置的二维码生成算法，根据所述URL，生成所述产品ID的防伪二维码
S205
接收终端扫描所述二维码触发的访问请求，获取所述访问请求携带的跟踪编码
S206
基于所述跟踪编码，查询所述跟踪编码对应的预置防伪信息，并对所述跟踪编码进行解码，以获取所述跟踪编码中的防伪信息
S207
当所述防伪信息与预置防伪信息不一致时，向所述终端发送异常提示信息
S208
当所述防伪信息与所述预置防伪信息一致时，获取所述访问请求携带的所述终端的目标ID信息和目标位置信息
S209
读取预置记录库中的ID信息和位置信息，将读取到所述ID信息和所述位置信息与所述目标ID信息和所述目标位置信息进行对比
S210
当所述ID信息与所述目标ID信息不一致，且所述位置信息与所述目标位置信息不一致时，向所述终端发送异常提示信息
S211

图5

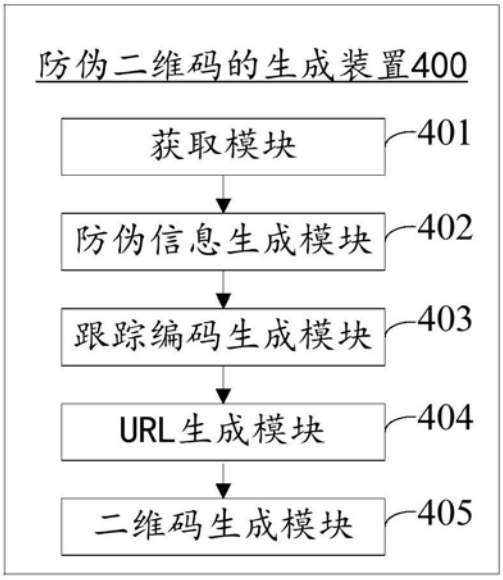

防伪二维码的生成装置400
获取模块
401
防伪信息生成模块
402
跟踪编码生成模块
403
URL生成模块
404
二维码生成模块
405

图6

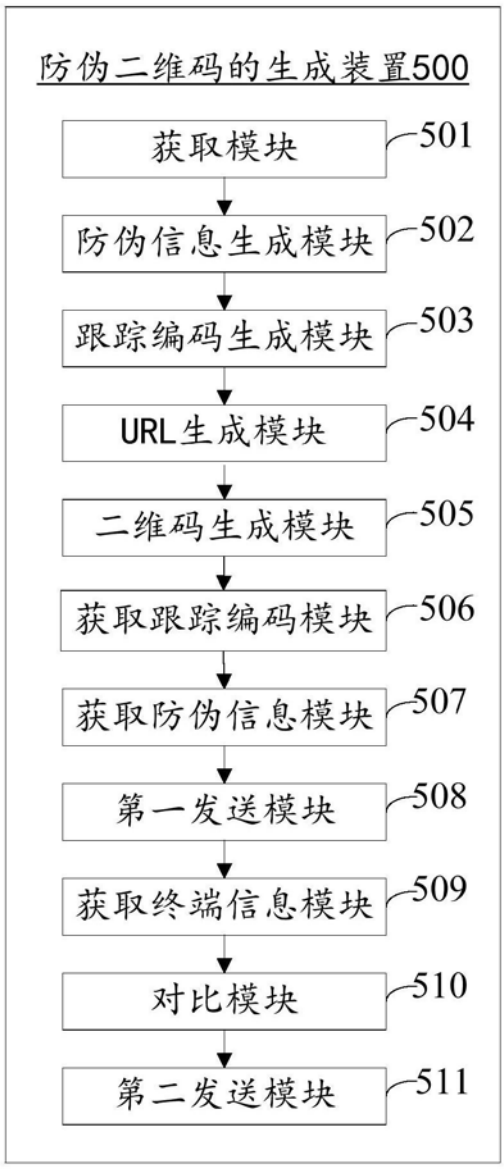

防伪二维码的生成装置500
获取模块
501
防伪信息生成模块
502
跟踪编码生成模块
503
URL生成模块
504
二维码生成模块
505
获取跟踪编码模块
506
获取防伪信息模块
507
第一发送模块
508
获取终端信息模块
509
对比模块
510
第二发送模块
511

图7

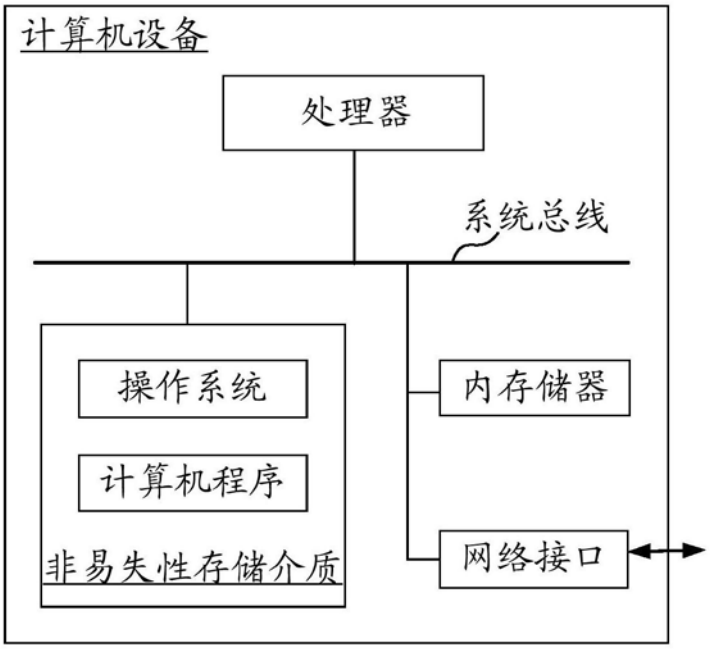


图8