



(12) 发明专利申请

(10) 申请公布号 CN 101887570 A

(43) 申请公布日 2010. 11. 17

(21) 申请号 201010233514. 3

(22) 申请日 2006. 02. 03

(30) 优先权数据

60/650, 364 2005. 02. 03 US

11/347, 424 2006. 02. 02 US

(62) 分案原申请数据

200680003972. X 2006. 02. 03

(71) 申请人 尧德品牌保护公司

地址 美国加利福尼亚州

(72) 发明人 E·格兰特 W·斯特林 M·塞尔夫

(74) 专利代理机构 北京市金杜律师事务所

11256

代理人 王茂华 李辉

(51) Int. Cl.

G06Q 30/00 (2006. 01)

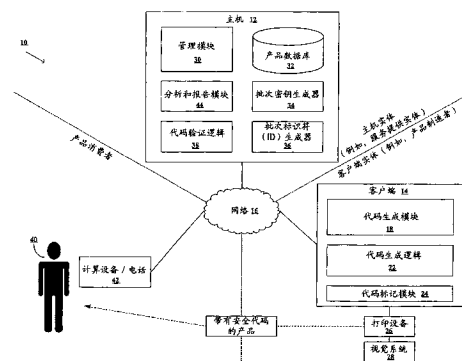
权利要求书 2 页 说明书 11 页 附图 7 页

(54) 发明名称

用于阻止产品伪造、转移和盗版的方法和系统

(57) 摘要

本申请公开了一种用于阻止产品伪造、转移和盗版的方法和系统。具体地，公开了一种方法，包括：接收生成唯一安全代码的集合的请求，每个单独的安全代码将被置于单独的产品项上；进一步接收与将在其上打印安全代码的产品相关联的产品数据；响应于请求由处理器生成安全代码，以及提供安全代码；以及响应于接收验证安全代码的请求，确定安全代码是否是所生成的安全代码中的一个；以及提供确定安全代码是否是所生成的安全代码中的一个的结果，以及进一步提供产品数据的至少部分。



1. 一种方法,包括:

接收生成唯一安全代码的集合的请求,每个单独的安全代码将被置于单独的产品项上;

进一步接收与将在其上打印所述安全代码的产品相关联的产品数据;

响应于所述请求由处理器生成所述安全代码,以及提供所述安全代码;以及

响应于接收验证安全代码的请求,确定所述安全代码是否是所生成的安全代码中的一个;以及

提供确定所述安全代码是否是所生成的安全代码中的一个的结果,以及进一步提供所述产品数据的至少部分。

2. 根据权利要求1所述的方法,其中与将在其上打印所述安全代码的产品相关联的产品数据包括:所述产品的预期目的地。

3. 根据权利要求1所述的方法,其中与将在其上打印所述安全代码的产品相关联的产品数据包括以下一个或者多个:通用产品代码(UPC)、产品描述、包装尺寸、数量、或者产品或包装图像。

4. 根据权利要求1所述的方法,其中与将在其上打印所述安全代码的产品相关联的产品数据包括以下一个或者多个:时间属性、位置属性、工作顺序、批号、制造日期、最迟使用日期、操作员姓名或者制造工厂。

5. 根据权利要求1所述的方法,其中提供先前接收的产品数据的至少部分依赖于已标识的请求者位置。

6. 根据权利要求5所述的方法,其中所述已标识的请求者位置是海关官员或者消费者之一。

7. 根据权利要求1所述的方法,进一步包括:

接收来自主机计算系统的批次标识;以及

其中生成所述安全代码包括:将所述批次标识与多个唯一标识符中的每一个相结合。

8. 根据权利要求1所述的方法,其中:

接收所述产品数据是由客户端计算系统执行的;

所述方法进一步包括:所述客户端计算系统向主机计算系统发送所述产品数据的至少部分,以及其中:

由所述主机计算系统执行以下两者:确定所述安全代码是否是所生成的安全代码中的一个,以及其中进一步提供所述产品数据的至少部分。

9. 一种其上存储有指令集的机器可读介质,当执行所述指令集时执行如下方法,包括:

接收生成唯一安全代码的集合的请求,每个单独的安全代码将被置于单独的产品项上;

进一步接收与将在其上打印所述安全代码的产品相关联的产品数据;

响应于所述请求,生成并提供所述安全代码;以及

响应于接收验证安全代码的请求,确定所述安全代码是否是所生成的安全代码中的一个,以及

提供确定所述安全代码是否是所生成的安全代码中的一个的结果,以及进一步提供所

述产品数据的至少部分。

10. 根据权利要求 9 所述的机器可读介质,其中与将在其上打印所述安全代码的产品相关联的产品数据包括:所述产品的预期目的地。

11. 根据权利要求 9 所述的机器可读介质,其中与将在其上打印所述安全代码的产品相关联的产品数据包括以下一个或者多个:通用产品代码(UPC)、产品描述、包装尺寸、数量、或者包装图像。

12. 根据权利要求 9 所述的机器可读介质,其中与将在其上打印所述安全代码的产品相关联的产品数据包括以下一个或者多个:时间属性、位置属性、工作顺序、批号、制造日期、最迟使用日期、操作员姓名或者制造工厂。

13. 根据权利要求 9 所述的机器可读介质,其中提供先前接收的产品数据的至少部分依赖于已标识的请求者位置。

14. 根据权利要求 13 所述的机器可读介质,其中所述已标识的请求者是海关官员或者消费者之一。

15. 一种系统,包括:

接收生成唯一安全代码的集合的请求的单元,每个单独的安全代码将被置于单独的产品项上;

进一步接收与将在其上打印所述安全代码的产品相关联的产品数据的单元;

响应于所述请求而生成并提供所述安全代码的单元;

响应于接收验证所述安全代码的请求、确定所述安全代码是否是所生成的安全代码中的一个的单元;以及

提供确定所述安全代码是否是所生成的安全代码中的一个的结果、以及进一步提供所述产品数据的至少部分的单元。

16. 根据权利要求 15 所述的系统,其中与将在其上打印所述安全代码的产品相关联的产品数据包括:所述产品的预期目的地。

17. 根据权利要求 15 所述的系统,其中与将在其上打印所述安全代码的产品相关联的产品数据包括以下一个或者多个:通用产品代码(UPC)、产品描述、包装尺寸、数量、或者包装图像。

18. 根据权利要求 15 所述的系统,其中与将在其上打印所述安全代码的产品相关联的产品数据包括以下一个或者多个:时间属性、位置属性、工作顺序、批号、制造日期、最迟使用日期、操作员姓名或者制造工厂。

19. 根据权利要求 15 所述的系统,其中提供先前接收的产品数据的至少部分依赖于已标识的请求者位置。

20. 根据权利要求 19 所述的系统,其中所述已标识的请求者位置是海关官员或者消费者之一。

## 用于阻止产品伪造、转移和盗版的方法和系统

[0001] 本申请是申请日为 2006 年 2 月 3 日、申请号为 200680003972.X 以及发明名称为“用于阻止产品伪造、转移和盗版的方法和系统”的中国专利申请的分案申请。

[0002] 相关申请的交叉引用

[0003] 本申请要求 2005 年 2 月 3 日提交的美国临时申请第 60/650,364 号的利益,其通过参考合并于此。

### 技术领域

[0004] 本发明一般地涉及反伪造措施,并且特别涉及用于验证产品并且从而阻止伪造转移和 / 或盗版的方法和系统。

### 背景技术

[0005] 在消费品工业中,伪造是重大和不断增长的问题。虽然时尚和奢侈品已经长时间地成为伪造的目标,但几乎任何牌子的产品都可以是伪造的对象。例如,诸如洗发水、汽车零件、婴儿配方以及甚至啤酒都已经是伪造的对象。伪造是难以检测、调查和量化的。因而,难以知道问题的全部范围。然而,通过某些估计,全世界贸易的百分之五到七之间是伪造货物,总计年价值超过 2500 亿美元。随着全球化的继续以及供应链进一步在缺乏检测并阻止伪造的能力和 / 或意愿的发展中国家中扩展,这个数字很可能增加。

[0006] 在传统的伪造方案中,个人或者个人的群体生产、包装以及试图出售带有欺骗性地代表产品的真实性和 / 或来源的目的的产品。在多数情况下,伪造品的质量低于伪造品设计效仿的原产品。因而,不知不觉地购买了伪造货物的消费者被欺骗了。在某些情况中,诸如对于药品、药物和汽车零件,当消费者不知不觉地购买了伪造品时,结果可能是致命的。

[0007] 伪造对于商业实体也具有重大的影响。可能伪造品对于公司所具有的最明显的负面影响是失去收入和利润。不明显但是也一样重要的是伪造可以引起公司的品牌价值的潜在损害。例如,由使用伪造品引起的一个被大肆宣传的负面事件可以对公司声誉引起不可估量的破坏。

[0008] 已经开发或者提出了用于阻止伪造的若干技术。例如,针对阻止伪造的某些技术包括:利用采用全息图、变色墨水、篡改标签、凹板墨和紫外线墨水的识别标记来给产品,标签或者产品包装作标记。然而,这个方法经常是无效的,因为识别标记很容易被伪造者复制,和 / 或消费者很难识别。

[0009] 阻止伪造的另一个方法是利用射频识别 (RFID) 标签。例如,通过当产品被初次包装时给它附着一个特定 RFID 标签,以后可以通过检验由 RFID 标签传达的唯一识别数据来验证产品。然而,给每个产品添加 RFID 标签增加了产品的整体成本。而且,检验 RFID 标签所需的设备(例如,RFID 传感器或者读取器)可以在产品的分配链中仅对于特定的实体是可获得的,并且几乎肯定的是对于产品的消费者不可获得。RFID 标签本身或者它们之内的代码也易遭伪造。因而,存在对于有效并且经济的反伪造系统的需要。

## 发明内容

[0010] 提供了用于检测并且阻止伪造的方法和系统。与本发明的一个实施例一致,用于阻止伪造的系统包括客户端和主机。客户端包括代码生成逻辑,其利用从主机接收的数据生成一批安全代码。一旦生成安全代码,则客户端指示打印设备将该批安全代码打印在一批产品上,在打印设备已经将安全代码打印在产品上之后,不保留安全代码。主机包括代码验证逻辑,其接收已经被打印在特定产品上的安全代码以及代码验证请求。从而,主机通过确定安全代码是否是由客户端生成的来验证安全代码。

## 附图说明

[0011] 本发明以示例的方式加以说明并且不限于所附的附图,其中相同的参考表示相似的元件,并且其中:

[0012] 图 1 描述了根据本发明的一个实施例的具有主机组件和客户端组件的反伪造系统;

[0013] 图 2 描述了根据本发明的一个实施例的用于生成多个将要被打印在产品上的多个唯一安全代码的方法;

[0014] 图 3 描述了根据本发明的实施例的用于验证已经在上面打印了安全代码的产品的方法;

[0015] 图 4 描述了根据本发明的实施例的与用于生成安全代码的方法相关的操作和数据流程;

[0016] 图 5 描述了根据本发明的实施例的与用于验证包含安全代码的产品的方法相关的操作和数据流程;

[0017] 图 6A 描述了根据本发明的实施例的包括字母数字文本的安全代码的例子;

[0018] 图 6B 描述了根据本发明的实施例的包括编码为图形符号的字母数字文本的安全代码的例子;

[0019] 图 7 描述了按照计算机系统的示例性方式的机器的概略图形表示,在其中可以执行用于引起机器执行任意一个或多个这里讨论的方法的指令集。

## 具体实施方式

[0020] 描述了用于检测并且阻止伪造的方法和系统。在下列描述中,为了解释的目的,提出许多特定的细节以达到提供本发明彻底的理解的目的。然而,对于本领域技术人员明显的是,没有这些特定细节,也可实现本发明。这里的描述和表示是由本领域那些经验丰富或者熟练的技术人员使用来向本领域的其他技术人员有效地传达他们工作的实质的手段。在某些示例中,为了避免不必要的使本发明的各个方面变得模糊,熟知的操作和组件不再详细描述。

[0021] 这里的参考“一个实施例”或者“实施例”意味着与实施例相关联地描述的特定特征、结构、操作或者其他特性可以被包括在本发明的至少一个实现中。然而,短语“在一个实施例中”在说明书中不同地方的出现不是必须指相同的实施例。

[0022] 本发明的实施例包括用于验证原产品并且从而检测以及阻止产品伪造的方法和

系统。在本发明的一个实施例中,用于检测伪造的系统包括主机组件和客户端组件。因而,客户端利用从主机接收的数据生成多个安全代码,并且然后指示打印设备将安全代码打印在消费产品上。然而,相对于以前所知的反伪造系统的是,在安全代码已经被打印在产品上之后,不保留安全代码。即,在安全代码已经被打印并且产品已经被置于商业流中后,主机和客户端都不在短期或者长期存储器中保留安全代码。而且,在本发明的一个实施例中,安全代码在它们被打印在产品上的地方生成。因而,安全代码不需要通过网络被传送,在网络上它们可能被例如网络数据包嗅探应用所损坏。

[0023] 如下面将进行的更加详细的描述,产品分配链中的产品消费者或者任何其他人可以通过仅将安全代码传送给主机来使其上已经打印了安全代码的产品的真实性得以检验。而且,广泛的多种设备和方法可以被用来将安全代码传送给主机用于验证。例如,可以使用电话通过说出安全代码,或者可选地,通过使用电话的按键式拨号盘输入安全代码从而将安全代码传送给主机。可选地,计算设备(例如,个人计算机、个人数字助理、移动电话,等)可以被用于将安全代码传送给主机。例如,可以使用键盘、电话键盘、照相机或者条形码读取器捕获安全代码,以及然后发送给主机。在主机已经接收并且验证了安全代码后,主机将验证操作的结果传送给消费者。

[0024] 本领域技术人员将会理解,本发明特别适用于品牌产品和商品。品牌产品可以包括任何具有可识别的来源(例如,制造商或者供应商)的产品。经常地,但是肯定不是总是的,使用诸如商标的专用名称或特征来标记品牌产品。在某些情况中,产品品牌可以通过产品或者商品的设计、形状或者颜色被辨认。品牌产品可以包括,但是绝不限于:医药品、化妆品、洗漱用品、护发品、营养品、玩具、烟草、食品、饮料、汽车零件、服饰和鞋类、计算机硬件和软件、电子设备、家庭用品、清洁产品、护目镜类和奢侈品。

[0025] 图1描述了根据本发明的一个实施例的反伪造系统10,具有主机组件12和客户端组件14。在本发明的一个实施例中,主机12可以由向一个或多个产品制造者提供反伪造服务的实体所维护和操作。因而,主机12可以通过网络16连接到任意数目的客户端14。例如,具有若干产品包装设备的产品制造商可以使用多个客户端14,每个单独的包装设备处有一个客户端14。类似地,主机12可以服务于与不同产品制造商相关联的多个客户端14。

[0026] 主机12和客户端14进行通信所使用的网络16可以是诸如因特网的开放网络或者专用网络。在本发明的一个实施例中,主机12和客户端14间的通信依靠安全通信协议完成,例如,诸如安全套接字层(SSL)或者传输层安全(TLS)。

[0027] 再次参考图1,客户端14包括代码生成模块18、代码生成逻辑22和代码标记模块24。代码生成模块18便于客户端14和客户端14的用户(例如,客户端用户)间交互。

[0028] 在本发明的一个实施例中,客户端用户可以通过输入指示所需一批安全代码的尺寸的数字来启动该批安全代码的生成。另外,代码生成模块18可以提示客户端用户输入与将要在上面打印安全代码的产品相关联的产品数据。例如,代码生成模块18可以提示客户端用户输入产品数据,诸如通用产品代码(UPC)、产品描述、包装尺寸和数量、包装图像,或者一些特定时间或位置属性,诸如工作顺序、批号、制造日期、最迟使用日期、操作员姓名或者制造工厂。输入到代码生成模块18中的产品数据连同生成安全代码的请求一起被传送到主机12。

[0029] 在验证操作期间(其联系下面图5的描述被更详细地描述),响应于代码验证请

求,由客户端用户输入的或者存储在主机上的产品数据或者产品数据的子集可以被显示或者被传送给供应链中的消费者或者其他入。而且,显示或者传送的特定产品数据可以取决于提交代码验证请求的人而改变。特别地,显示或者传送的产品数据可以依据整个供应链或者商业流中人的位置而变化。例如,提交代码验证请求的海关官员可以被呈现多于消费者的不同的产品数据。

[0030] 如下面参考图 4 的描述更详细描述,代码生成逻辑 22 利用从主机 12 接收的数据生成打印在产品上的安全代码。在本发明的一个实施例中,代码标记模块 24 控制传输安全代码到打印设备 26,其可以将安全代码直接打印在产品上,或者可选地,打印在产品标签或者产品包装上。因而,代码标记模块 24 可以确认安全代码被正确地从主机 12 传输到打印设备 26。另外,代码标记模块 24 可以保持运行已经从客户端 14 传输到打印设备 26 的安全代码数目和 / 或已经被打印的安全代码的数目的连续计数。

[0031] 打印设备 26 可以是适合在产品、标签或者产品包装上打印安全代码的任意类型的打印系统。例如,打印设备 26 可以包括高速工业喷墨打印机(带有可见或者隐形墨水)、热转移式打印机(带有可见或者隐形色带)、激光标记器或者其他工业标记系统。在特定的实施例中,特殊隐形墨水或者其他相关技术可以被使用来利用隐形安全代码隐式地标记产品。打印设备 26 由这些打印技术的任意组合组成。本领域技术人员将会理解,打印设备规范将基于消费者的性能要求、包装或者产品的基底材料以及操作环境,并且通常将反映这样的打印或者标记系统中的目前技术。

[0032] 在本发明的一个实施例中,安全代码被打印在防篡改密封上。因而,防篡改密封可以置于产品上,使得当打开或者使用产品时,毁坏该防篡改密封。因而,一旦毁坏,安全代码不能被重新使用。

[0033] 在本发明的一个实施例中,打印设备 26 可以连接到或者集成到视觉系统 28 或者其他成像设备中。视觉系统 28 可以当安全代码被打印时扫描或者读取每个安全代码以检测是否发生打印问题并且确保全部的打印品质等级符合要求。因而,当在特定安全代码的打印中检测到一个错误时,视觉系统 28 可以通过通知客户端 14 或者主机 12 标记该安全代码,或者丢弃低品质打印的安全代码。视觉系统 28 可以通过使用“机器视觉”来实现,诸如光学或者非接触读取器,其具有当安全代码被打印在产品、标签或者产品包装上时检测它们的物理属性的能力。视觉系统 28 协同其他过程控制方式确保只有高品质的安全代码被打印在产品或者包装上,同时保持极低的丢弃率以维持装箱或者包装线上的生产率和吞吐量。

[0034] 如图 1 中所描述的,打印设备 26 和视觉系统 28 是与客户端 14 分开的。本领域技术人员将会理解,在可选的实施例中,打印设备 26 可以与图 1 中的客户端集成在一起。类似地,如图所示,代码标记模块 24 与客户端 14 集成在一起。本领域技术人员将会理解,在可选的实施例中,代码标记模块 24 可以与打印设备 26 集成在一起。在本发明的一个实施例中,客户端 14 可以以分布式来实现,使得一个或多个客户端组件在地理上是分开的。例如,在本发明的一个实施例中,代码生成模块 18 可以位于商业总部,而一个或多个其他组件(包括打印设备)位于包装设备处。在分布式的实施例中,一个代码生成模块 18 可以被集成以支持并且与多个代码标记模块 24 和 / 或打印设备 26 一起工作。因而,当制造者具有多个包装设备时,可以实现分布式的实施例。

[0035] 反伪造系统 10 的主机 12 包括管理模块 30。相似于客户端 14 的代码生成模块 18，管理模块 30 便于主机 12 和主机用户间的交互。

[0036] 主机 12 包括批次标识符（批次 ID）生成器 36 和批次密钥生成器 34。如下面更加详细描述，响应于接收客户端请求生成安全代码，批次 ID 生成器 36 生成用于安全代码集合的批次 ID 并且批次密钥生成器 34 生成相关联的批次密钥（也称为种子数）。批次 ID 和批次密钥与客户端请求相关联，并且连同利用客户端请求所接收的产品数据一起由主机 12 存储在例如产品数据库 32 中。另外，主机 12 将批次 ID 和批次密钥传送给客户端 14，其利用批次 ID 和批次密钥生成被打印在产品上的唯一安全代码。

[0037] 主机 12 也包括代码验证逻辑 38。如下面结合图 5 的描述更详细描述，代码验证逻辑 38 接收并验证已经打印在产品上的安全代码。例如，在安全代码已经打印在产品上之后，供应链或者商业流中的消费者或者其他人可以出于验证的目的将安全代码传送给主机 12。如果主机 12 确定安全代码是可信的，则主机 12 可以将此报告给消费者。

[0038] 与本发明的实施例一致，各种方法和设备可以被用来将安全代码告知主机 12，用于验证。例如，在一个实施例中，消费者 40 可以利用基于电话的服务（例如，语音，短消息系统（SMS），支持 web 的应用）、个人计算机、个人数字助理、可视电话或者其他带有数据通信的计算设备 42，来将代码验证请求（包括安全代码）传送给主机 12。在安全代码被传送给主机 12 之后，代码验证逻辑 38 将确认安全代码的真实性。在本发明的一个实施例中，主机 12 可以使用包括与产品有关的关键属性的消息回应代码来验证请求。例如，来自于主机 12 的响应包括特定商品的描述，包括品牌名称、尺寸或者数量、过期日期、制造日期，制造地点、批号或者任何其它潜在的相关数据。

[0039] 在本发明的一个实施例中，主机 12 包括分析和报告模块 44。分析和报告模块 44 具有两个主要功能。第一，分析组件通过追踪和分析代码验证请求来提供用于识别潜在欺骗活动的机制。例如，每次接收到验证特定安全代码的请求时，分析组件进行记录，并且当可能时，记录接收的每个请求的来源（例如，人、地理位置、或者其他设备标识符，诸如因特网协议地址）。因而，通过分析利用代码验证请求接收的安全代码，分析组件能够检测可以指示伪造活动的可疑图案，例如，如果可信的安全代码被复制并且被用于一批伪造品上，那么很可能多个消费者试图验证相同的安全代码（例如，复制的安全代码）。通过检测可疑图案，分析和报告工具 44 可以通知制造商的品牌安全人员去监视供应链的特定点上的活动。

[0040] 分析和报告模块 44 的另一个主要功能是报告功能。在本发明的一个实施例中，模块 44 的报告组件提供用于报告可疑活动的机制，也是通常的商业报告。报告可以提出计划给出了解供应链中的欺骗或者可疑活动的相关信息范围，并且允许品牌安全人员采取快速的预防性行动。另外，报告组件可以生成商业报告，其包括与用于不同产品的验证活动有关的格式化的数据。可以通过客户端、主机或者此两者来定制报告功能。在一个实施例中，可以建立用于分析和报告模块 44 的报告规则和警告，如果已经触发了伪造品警告，例如通过检测指示出安全代码已经被复制或者克隆的高可能性的代码验证请求的图案，则分析和报告模块 44 自动警告品牌安全人员。

[0041] 本领域技术人员将会理解，图 1 所示的反伪造系统 10 被提供作为本发明的一个例子或者实施例，而不意味在本质上是限制的。系统可以包括其他逻辑和功能或者模块的组件，没有提供它们的描述以避免使本发明不必要的模糊。



[0042] 图 2 描述了根据本发明的一个实施例的用于生成多个将要被打印在产品上的唯一的安全代码的方法 50。如图 2 所示的,在或者由客户端 14 执行的与方法 50 相关的操作(即,虚线 51 的左面)与那些在或者由主机 12 执行的操作分离开来。在操作 52 处,客户端 14 接收用户发起的请求以生成用于特定产品的多个安全代码。例如,可以经由客户端 14 的代码生成模块 18 接收用户发起的请求。而且,用户发起的请求可以包括与将在上面打印安全代码的产品相关的数据,以及指示将被生成和打印的安全代码的数量的数目。

[0043] 在接收了用户发起的请求之后,客户端 14 在操作 54 确定客户端请求并且将客户端请求传送给主机 12。例如,在本发明的一个实施例中,客户端 14 可以抽取由客户端用户输入的产品数据的一部分,并且将抽取的产品数据连同用户输入的数目包括于客户端请求中,其中该数目指示将要被生成和打印的安全代码的数量。然后,客户端 14 将客户端请求(例如,通过网络 16)传送给主机 12。在本发明的一个实施例中,对客户端 14 与主机 12 间的通信进行加密或者保护。

[0044] 在操作 56,主机 12 接收客户端请求。响应于接收客户端请求,在操作 58,主机 12 生成批次标识符和批次密钥(或者种子数)。批次 ID 可以保证批次 ID 与所有以前用过的批次 ID 不同的任意方式生成,诸如简单数值级数、确定性伪随机序列、或者一系列随机生成值,其中副本被移除。批次密钥可以由伪随机序列、硬件随机数生成器或者生成难以预知的密钥的任何方法生成。本领域技术人员将会理解,为了保证安全代码的完整性,批次密钥以不能为试图生成伪造代码的个人或者系统所预知的方式生成是重要的。批次密钥也应该是唯一的,以阻止重复的安全代码由客户端 14 生成。批次 ID 和批次密钥连同从客户端 14 接收的产品数据被存储在主机 12 的产品数据库 32 中。然后,在生成批次 ID 和批次密钥后,在操作 60 处,主机 12 将批次 ID 和批次密钥传送给客户端 14。

[0045] 在本发明的一个实施例中,可选的加密密钥 94(也叫加扰 ID),连同批次 ID 和批次密钥一起从主机 12 传送给客户端 14。如下更详细描述,加密密钥 94 指示特定的加扰或者加密方法,其由客户端 14 在安全代码生成期间并且由主机 12 在安全代码验证期间使用。可选地,除了将加密密钥 94 从主机 12 传递到客户端 14,可以配置主机 12 和客户端 14,以利用预定的加扰或者加密方法。

[0046] 在操作 62 处,在从主机 12 接收到批次 ID 和批次密钥之后,客户端 14 利用批次 ID 和批次密钥,以在操作 64 处生成多个安全代码。另外,在操作 64 处,客户端 14 指示打印设备 26 在产品上打印安全代码,而不将安全代码保留于安全代码库中(例如,数据库或者记录介质)。因此,在客户端 14 已经指示打印设备 26 将安全代码打印在单独的产品上之后,客户端 14 和主机 12 都不保留安全代码。即,安全代码不保留在存储器中并且不写到磁盘存储器中。安全代码也不需要传输到主机 12。如果未经授权的人获取进入客户端 14 或者主机 12,这阻止了安全代码被危害。并且,由于安全代码在打印位置生成,所以不存在安全代码在传送(例如,通过网络)到打印位置中将被破坏的风险。客户端 14 在安全代码已经被打印后不保留批次密钥,因此没有做出从客户端 14 到主机 12 的新的请求的情况下,不能产生另外的安全代码。

[0047] 在用于该批的所有安全代码的打印完成后,可选地,客户端 14 将被打印的安全代码的实际数目传送给主机 12,如果中断代码生成或者打印或者如果制造的产品数目少于预期,则所述实际数目可以少于最初请求的数目。

[0048] 图 3 描述了根据本发明的实施例的用于验证其上已经被打印了安全代码的产品的方法 70。如图 3 所示的,在或者由主机 12 执行的与方法 70 相关的操作(即,虚线 71 的右面)与由那些在产品供应或产品分配链中的消费者或者其他人所执行的操作分离开来。在本发明的一个实施例中,当消费者识别所怀疑的产品包装上的安全代码时,用于验证产品的方法 70 在操作 72 处开始。

[0049] 接下来,在操作 74 处,消费者将包括安全代码的代码验证请求传送给主机 12。在本发明的不同实施例中,操作 74 可以以若干种方式中的一种来完成。如果安全代码被作为字母数字文本提供在产品、标签或者产品包装上,那么消费者可以使用任何可以使消费者能够输入字母数字文本的通信设备来将安全代码传送给主机的代码验证逻辑 38。例如,消费者可以使用执行在诸如个人计算机、个人数字助理(PDA)、移动电话或者任何其他类似的设备的计算设备上的基于 Web 的应用,以将安全代码通过网络传送给主机 12。在本发明的一个实施例中,主机 12 的代码验证逻辑 38 可以包括语音识别模块、计算机电话应用,或者综合话音响应单元(未示出)。因而,消费者可以向电话说出字母数字安全代码,以将安全代码传送给主机 12。在本发明的特定实施例中,安全代码可以是已经被编码为图形符号的字母数字文本,诸如数据矩阵或者其他条形码。在这样的情况下,消费者可以利用带有图像读取或者图像捕获机制的设备以将安全代码告知主机 12。例如,照相机或者扫描仪可以用来捕获安全代码的图像(例如,图形符号),然后将其传送给主机。在本发明的特定实施例中,图形符号在被告知主机 12 之前,可以对其进行解码,以产生字母数字文本。可选地,在本发明的特定实施例中,主机 12 的代码验证逻辑 38 可以包括能够将图形符号的扫描图像解码为字母数字文本的解码组件。

[0050] 再次参考图 3 中描述的方法 70,在操作 76 处,主机 12 接收代码验证请求和安全代码。在操作 78 处,主机 12 验证安全代码。在参考图 5 的下面描述中提供验证操作的例子。本领域技术人员将会理解,验证操作可以取决于特定的实现而变化。然而,与本发明一致,主机和客户端都不在安全代码已经被打印在产品上之后存储它。因此,代码验证逻辑 38 能够验证安全代码,而没有访问存储在仓库或者数据库中的安全代码的副本。

[0051] 在安全代码已经由主机 12 的代码验证逻辑 38 验证之后,在操作 80 处,主机 12 可以将验证操作的结果传送给消费者。在本发明的一个实施例中,将以与从消费者接收代码验证请求和安全代码同样的方式,来传送验证操作的结果。例如,如果通过电话呼叫收到请求,那么自动计算机电话应用可以将操作结果通过电话传送给消费者。可选地,在本发明的一个实施例中,可以使用不同于用来接收安全代码的通信方式来传送验证结果。在任何情况下,在操作 82 处,消费者接收验证操作的结果。

[0052] 本领域技术人员将会理解,在前面的例子中,可以由计算设备实际执行归结于消费者的操作。例如,借助于某些计算设备或者电话将验证过程的结果传送给消费者。另外,本领域技术人员将会理解,可以以硬件、软件或者它们的任意组合来实现这里描述的功能组件、模块和逻辑。

[0053] 图 4 描述了根据本发明的实施例的与用于生成安全代码的方法相关联的操作和数据流。在图 4 中描述的操作作用在图 2 中描述的方法 50 的客户端侧操作 64 的一个例子。因而,在发起客户端请求以生成安全代码之后,客户端 14 的代码生成逻辑 22 从主机 12 接收数据。具体地,从主机 12 接收的数据包括三部分:批次 ID 92、批次密钥 90 和可选加密

密钥 94。另外,由序列号生成器 98 生成的序列号 96,其中序列号生成器 98 是客户端的代码生成逻辑 22 的一部分,从主机 12 接收的数据的三部分被用于生成安全代码。

[0054] 生成安全代码的操作开始于序列号 96、批次 ID 92 和批次密钥 90 (其也称为种子数)。序列号 96 是通过批次 ID 92 所识别的批次内产品的唯一标识符。序列号 96 可以由客户端 14 以保证该序列号与在该批中所有以前生成的序列号不同的方式生成,诸如简单数值级数 (progression)、确定性伪随机序列或者一系列随机生成的值,其中副本被移除。

[0055] 确认值 102 通过将批次 ID 92 和序列号 96 中的一个或者多个与批次密钥 90 进行组合来产生。之后,确认值可以被用于确定产生的安全代码 112 的真实性。在图 4 中示出的本发明的一个实施例中,批次密钥 90 作为种子被用于伪随机数生成器 100 生成用作确认值 102 的伪随机数。在已经生成确认值 102 后,可选地,由加密逻辑 104 加扰和 / 或加密序列号 96、批次 ID 92 和确认值 102。本领域技术人员将会理解,可以使用广泛的各种众所周知的加密 / 解密算法。例如,在本发明的一个实施例中,利用简单置换算法来加密数据。

[0056] 在本发明的一个实施例中,由加密逻辑 104 使用来加密数据 (例如,序列号 96、批次 ID 92 和确认值 102) 的加密算法与加密密钥 94 相关联。例如,在本发明的一个实施例中,加密逻辑 104 能够执行广泛的各种加密算法。因而,从主机 12 接收的加密密钥 94 指令或指示加密逻辑 104 使用特定的加密算法加密序列号 96、批次 ID 92 和确认值 102。因此,在验证操作期间,最初选择和分配加密密钥 94 的主机 12 将能够解密加密的数据 106 以实现序列号 96、批次 ID 92 和确认值 102。在本发明的一个实施例中,可以在主机将批次 ID 92 和批次密钥 90 传送给客户端的时候生成和分配加密密钥 94。可选地,可以在请求生成安全代码之前分配加密密钥 94。例如,在本发明的一个实施例中,可以基于每个客户端 14 分配加密密钥 94,使得每个客户端具有其自己的主机 12 知道的加密密钥 94。

[0057] 在序列号 96、批次 ID 92 和确认值 102 已经被加密以形成加密的数据 106 之后,可选的加密密钥插入逻辑 108 可以将加密密钥 94 的所有或者部分插入到加密的数据 106 中,以完成安全代码 110 的生成。例如,加密密钥 94 可以在已知位置处插入加密的数据 106。因此,在验证操作期间,主机 12 的代码验证逻辑 38 可以从安全代码中的已知位置抽取加密密钥 94。

[0058] 一旦加密密钥 94 被插入加密数据 106,安全代码 110 就准备好被打印在产品、标签和产品包装上。在本发明的一个实施例中,产生的安全代码可以是十六个字母数字字符的序列。例如,在图 4 中,安全代码 110 被示出为十六个字母数字字符的字符串 112。可选地,在本发明的一个实施例中,字母数字字符可以被编码为图形符号,诸如在图 6B 中描述的数据矩阵。在任意一种情况中,在安全代码由代码生成逻辑 22 生成之后,代码标记模块 24 控制并且管理安全代码到打印设备 26 的传输,以及安全代码实际打印在产品、标签或者产品包装上。

[0059] 再次参考图 4,在第一安全代码已经生成之后,代码生成操作通过生成用于该批的下一个序列号 114 而继续。为了生成对应于第二序列号的第二安全代码,通过将第二序列号和 / 或批次 ID 与批次密钥进行组合来产生第二确认值。在本发明的一个实施例中,随机数生成器 100 迭代运行多次,此数等于序列号。即,在第一过程 (pass) 期间生成的伪随机数被用作输入 (例如,种子) 进入伪随机数生成器 100 用于第二过程。因而,伪随机数生成器 100 运行两次以生成针对第二安全代码的确认值,第二安全代码与第二序列号相关联,并且

伪随机数生成器 100 运行三次以产生针对第三安全代码的确认值, 第三安全代码与第三序列号相关联, 以此类推, 直到已经生成所有安全代码。当生成的序列号和相应的安全代码数量等于由客户端最初请求的安全代码数目时, 代码生成操作完成。

[0060] 图 5 描述了根据本发明实施例的与用于验证包含安全代码的产品的方法相关联的操作和数据流。图 5 中描述的操作作用在图 3 中描述的方法 70 的主机侧操作 78 的一个例子。

[0061] 如图 5 中描述的, 验证操作开始于打印的安全代码 112。例如, 在图 5 中, 安全代码是 16 个字符和数字的组合。首先, 可选的加密密钥抽取逻辑 116 从安全代码 112 抽取加密密钥 94。因为代码生成逻辑 22 将加密密钥 94 插入到安全代码中的已知位置中, 代码验证逻辑 38 已经了解了安全代码 112 中的加密密钥 94 的位置。作为抽取加密密钥 94 的结果, 安全代码被减小到加密的数据 106 (例如, 序列号 96, 批次 ID 92 和确认值 102)。

[0062] 在加密密钥 94 已经被抽取之后, 加密密钥 94 被用作到解密逻辑 118 的输入以将加密的数据 106 解密为其组成部分, 例如, 序列号 96、批次 ID 92 和确认值 102。接下来, 在查询操作 120 中使用批次标识符 92 确定被使用来生成确认值 102 的批次密钥 90。批次密钥 90 的副本与批次 ID 92 和任何作为初始生成安全代码请求的一部分而从客户端 14 接收的产品数据存储在主机 12 处, 其中批次密钥 90 在主机 12 处响应于客户端生成安全代码的请求而初次生成。因此, 一旦批次 ID 92 被确定, 代码验证逻辑 38 可以查询批次密钥 90, 以及任何与批次 ID 92 相关联的产品数据。

[0063] 最后, 主机 12 使用与客户端 14 相同的方法, 通过将序列号 96 和 / 或批次 ID 92 与批次密钥 90 进行组合, 来产生第二确认值 124。在本发明的一个实施例中, 在批次 ID 92 被用于查询批次密钥 90 后, 批次密钥 90 被用于第二伪随机数生成器 122 的种子, 其使用与客户端 12 的伪随机数生成器 100 相同的逻辑。第二伪随机数生成器 122 然后迭代运行等于序列号 96 的次数, 使得每个过程使用先前过程的结果 (例如, 产生的伪随机数) 作为种子。产生的伪随机数被用作第二确认值 124, 然后, 其与由解密逻辑 118 解密的第一确认值 102 比较。如果确认值 102 和 124 相同, 那么主机 12 报告安全代码 112 是可信任的。然而, 如果确认值 102 和 124 不相同, 主机 12 报告安全代码 112 是不可信任的。

[0064] 在本发明的一个实施例中, 响应于消费者或者在产品的分配链中的其他人提交代码验证请求给主机, 与批次 ID 相关联的产品数据可以被传送给该消费者或者该人。例如, 在本发明的一个实施例中, 传送给消费者的产品数据可以表示针对给定产品的分配目的地 (例如, 地理位置或者零售商店)。即, 产品数据可以表示针对特定产品在分配链中的最终目的地。因而, 消费者可以确定是否产品已经被从它的初始分配的目的地转移了。在本发明的另一实施例中, 传送给消费者的产品数据可以包括与制造数据相关联的数据, “最迟使用” 或者 “最迟出售” 日期。因而, 消费者可以确定是否产品分配链中有人已经通过改变与产品相关联的数据而篡改了产品包装。通常, 在代码验证请求期间通过提供产品数据, 涉及产品的多个方面可以被验证。

[0065] 图 6A 和图 6B 描述了根据本发明实施例的安全代码的例子。在本发明的一个实施例中, 安全代码可以是十六个字母数字字符的字符串, 其中字符由数字和字母组成, 诸如图 6A 中所示的安全代码 130。通过使用十六个字母数字字符串的不同组合, 可以生成多于百万、十亿, 十亿 (1024) 个唯一安全代码。然而, 本领域技术人员将会理解, 本发明可选的

实施例可以使用的安全代码在长度上是多于或少于十六个字符的,并且可以使用利用整个 ASCII 字符集的安全代码。

[0066] 图 6B 说明了表示为图形符号的安全代码 132。具体地,在图 6B 中所示的安全代码 132 是被称为数据矩阵的特定机器可读取图形符号。数据矩阵是二维矩阵条形码,其由以正方形或者矩形图案排列的黑和白方形模块组成。类似于传统的条形码,数据矩阵可以由机器读取,诸如矩阵条形码读取器。将安全代码的字母数字表示编码为图形符号,诸如图 6B 的数据矩阵 132,提供了几个优势。第一,纠错和冗余是内置于数据矩阵 132 的。因此,如果如数据矩阵所表示的安全代码被部分损坏,则安全代码仍旧是可读的。另一个优势是数据矩阵的小印记或者尺寸。数据矩阵可以在三乘三毫米的正方形内编码多达 50 个字符,其可以被分散地置于产品、标签或者产品包装上。最后,数据矩阵可以由机器快速并且容易地读取。当然,本领域技术人员将会理解,在各种可选的实施例中,可以使用其他图形符号方法来编码安全代码,例如,诸如与 PDF417 或者 QR 代码标准一致的条形码字体。

[0067] 在本发明的一个实施例中,两个版本的安全代码 130 和 132 都可以被包括在产品、标签或者产品包装上。例如,安全代码 130 的字母数字表示和安全代码 130 的图形符号表示可以一起出现在产品、标签或者产品包装上。这提供了范围广泛的用于读取并且将安全代码传送给主机 12 用来验证的可能的的方法和机制。

[0068] 在本发明的一个实施例中,当需要额外的安全性时,可以使用隐蔽的方式将安全代码应用或者打印在产品、标签或者产品包装上,使得消费者认识不到安全代码的存在。例如可以使用特定隐形墨水或者其他基于化学品的应用,将安全代码应用在产品、标签或者产品包装上,其中该应用使得安全代码对于消费者不可见。根据被使用来应用安全代码的隐形墨水或者化学品的类型,读取安全代码可能需要施加热、紫外线、或者化学品。当供应或者分配链中的不同于消费者的某些人很可能会验证产品时,可以利用这个方法。例如,可以提供隐式的安全代码,用于由海关官员验证产品的目的。

[0069] 图 7 示出了计算机系统 300 的示例性形式中机器的概略的图形表示,在其中可以执行用于使机器执行任意一个或多个这里讨论的方法的指令集。在可选的实施例中,机器可以作为独立的设备操作或者可以被连接到(例如,通过联网)其他机器。在一个联网部署中,机器可以在客户端-服务器网络环境中在服务器(例如,主机 12)或者客户端 14 机器的能力内操作,或者在对等(或者分布式)网络环境中作为对等机器。机器可以是服务器计算机、客户端计算机、个人计算机(PC),平板 PC、机顶盒(STB)、个人数字助理(PDA)、蜂窝电话、Web 设备、网络路由器、交换机或者桥接器、或者能够执行指定由该机器所采取的动作的指令集(顺序的或者其它)的任何机器。此外,虽然仅描述了单个机器,但是术语“机器”也应该被采用以包括独立地或者联合地执行指令集(或者多个集合)以执行任意一个或多个这里讨论的方法的任何机器的集合。

[0070] 示例性的计算机系统 300 包括处理器 302(例如,中央处理单元(CPU)、图形处理单元(GPU)或者两者)、主存储器 304 和非易失性存储器 306、它们通过总线 308 彼此通信。计算机系统 300 还包括视频显示单元 310(例如,液晶显示器(LCD)或者阴极射线管(CRT))。计算机系统 300 也包括字母数字输入设备 312(例如,键盘)、指针控制设备 314(例如,鼠标)、盘驱动单元 316、信号生成设备 318(例如,扬声器)和网络接口设备 320。

[0071] 盘驱动单元 316 包括机器可读取介质 322,其上存储了一个或多个包含任意一个

或多个这里描述的方法或者功能的指令集（例如，软件 324）。在由计算机系统 300 执行它时，软件 324 也可以完全或者至少部分地驻留在主存储器 304 中和 / 或处理器 302 中，主存储器 304 和处理器 302 也构成机器可读取介质。软件 324 还可以经由网络接口设备 320 通过网络 326 传输或者接收。

[0072] 尽管机器可读取介质 322 在示例性实施例中所示出作为单个介质，但术语“机器可读取介质”应该被采用以包括存储一个或多个指令集的单个介质或者多个介质（例如，集中的或者分布的数据库、和 / 或相关的缓存和服务器等）。术语“机器可读取介质”还应该被采用以包括任何能够存储、编码或者携载用于由机器执行的并且使得机器执行本发明的任意一个或多个方法的指令集的介质。因而，术语“机器可读取介质”应该被采用以包括，但是不限于，固态存储器、光和磁介质以及载波信号。

[0073] 因此，已经描述了用于阻止伪造的方法和系统。尽管本发明已经参考特定的示例性实施例得以描述，但是明显地，在不偏离本发明的更广泛的精神和范围的情况下，可以对这些实施例做出各种修改和改变。因而，说明书和附图应该被当作说明性而不是限制性意义。

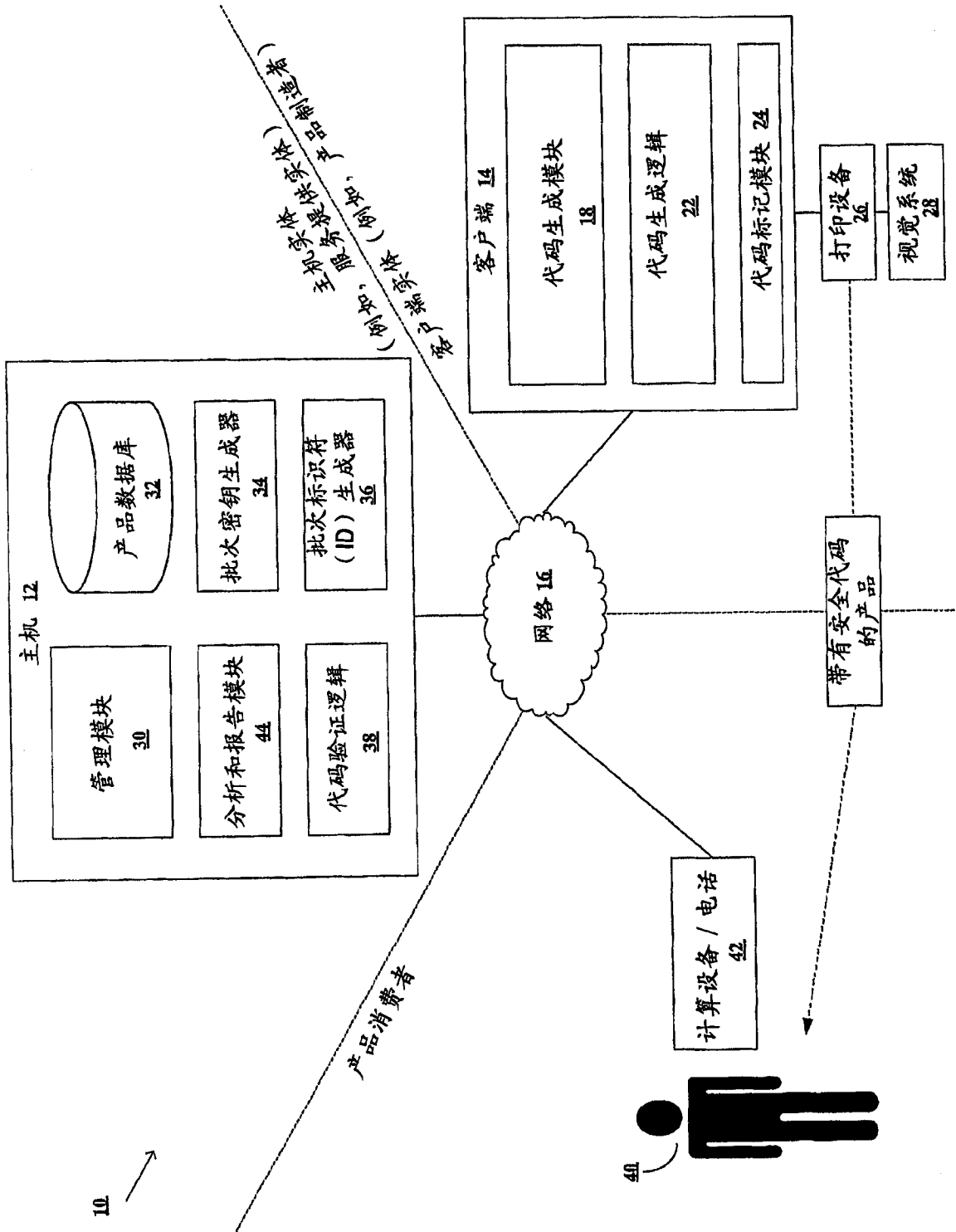


图 1

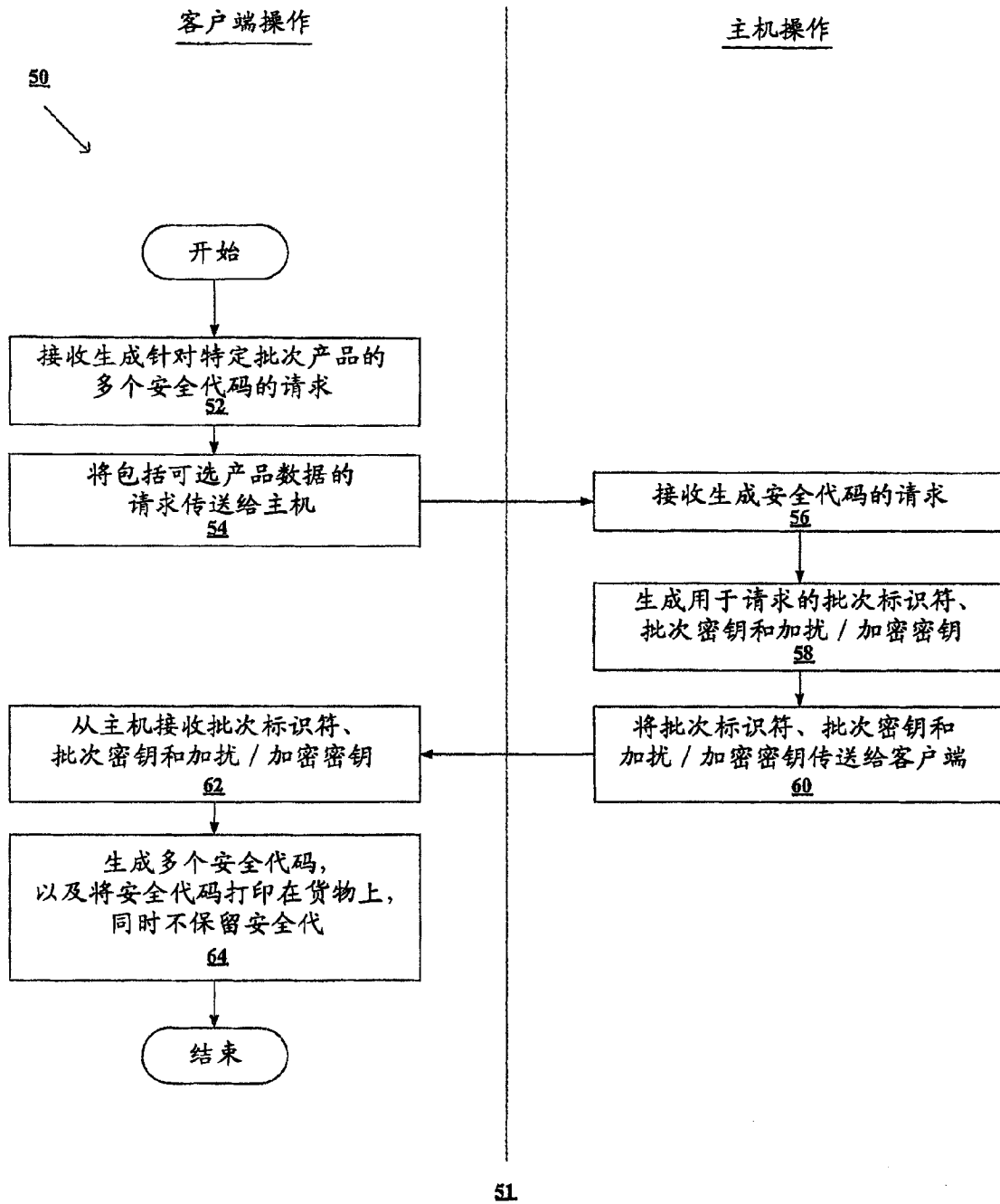


图 2



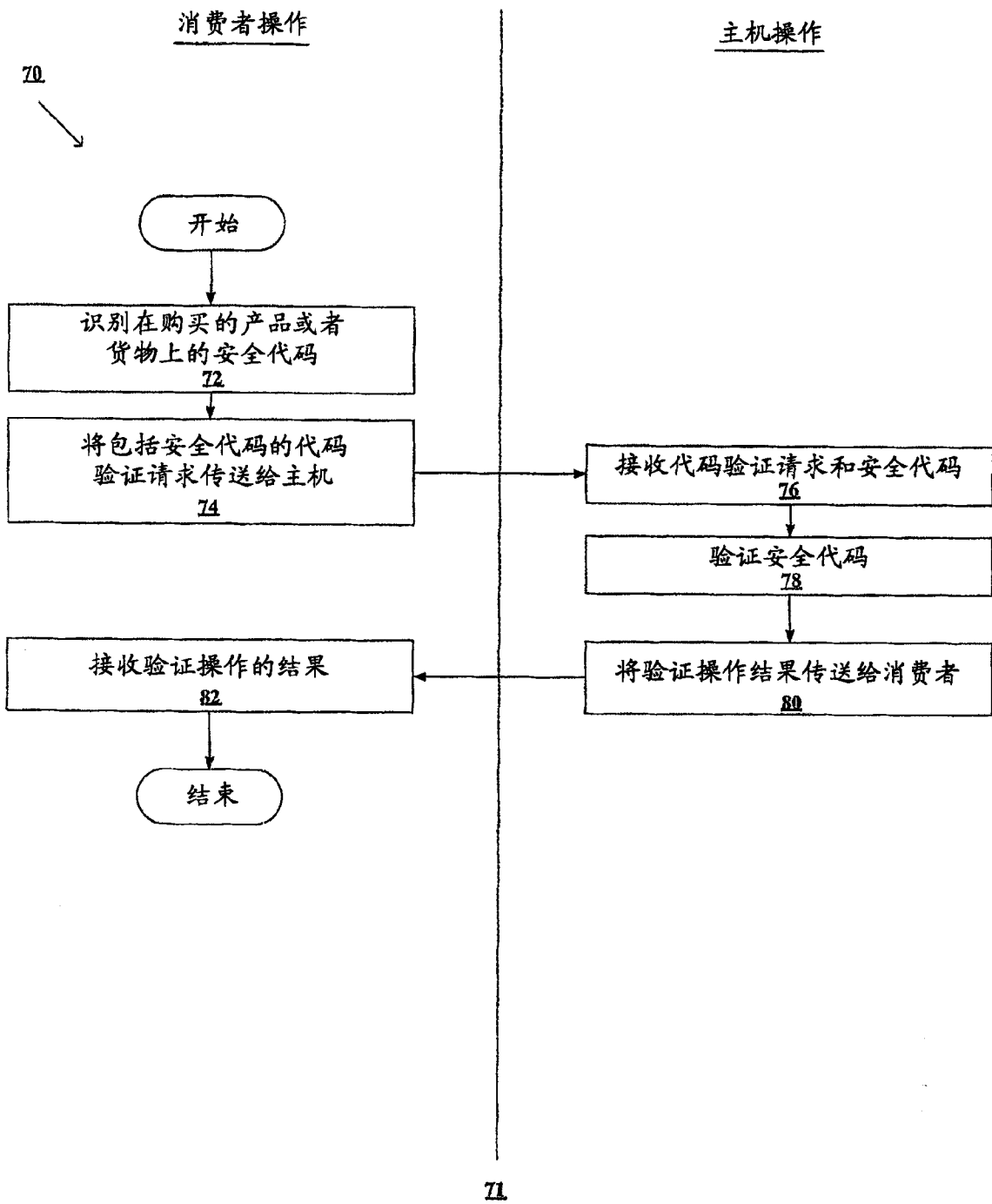


图 3

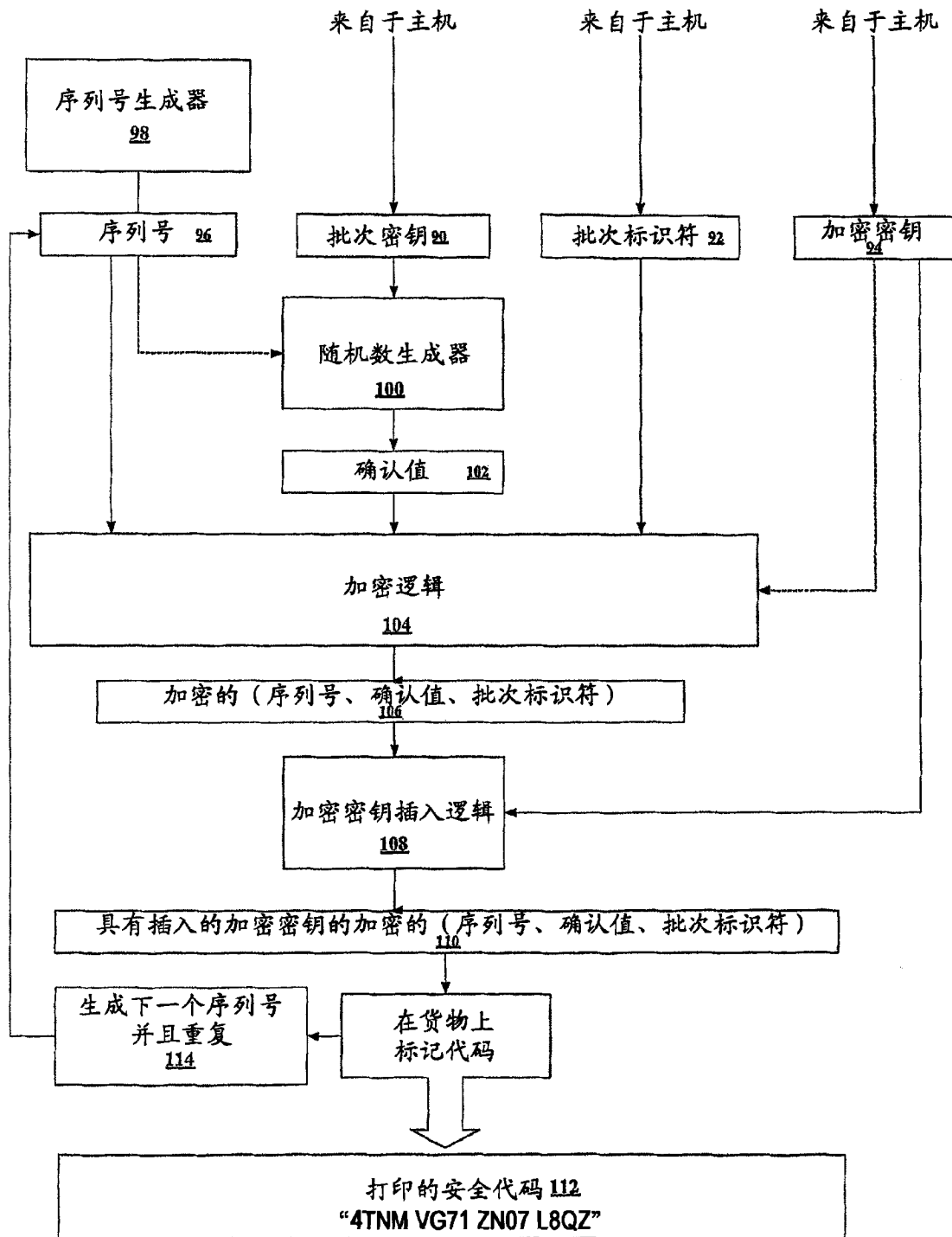


图 4

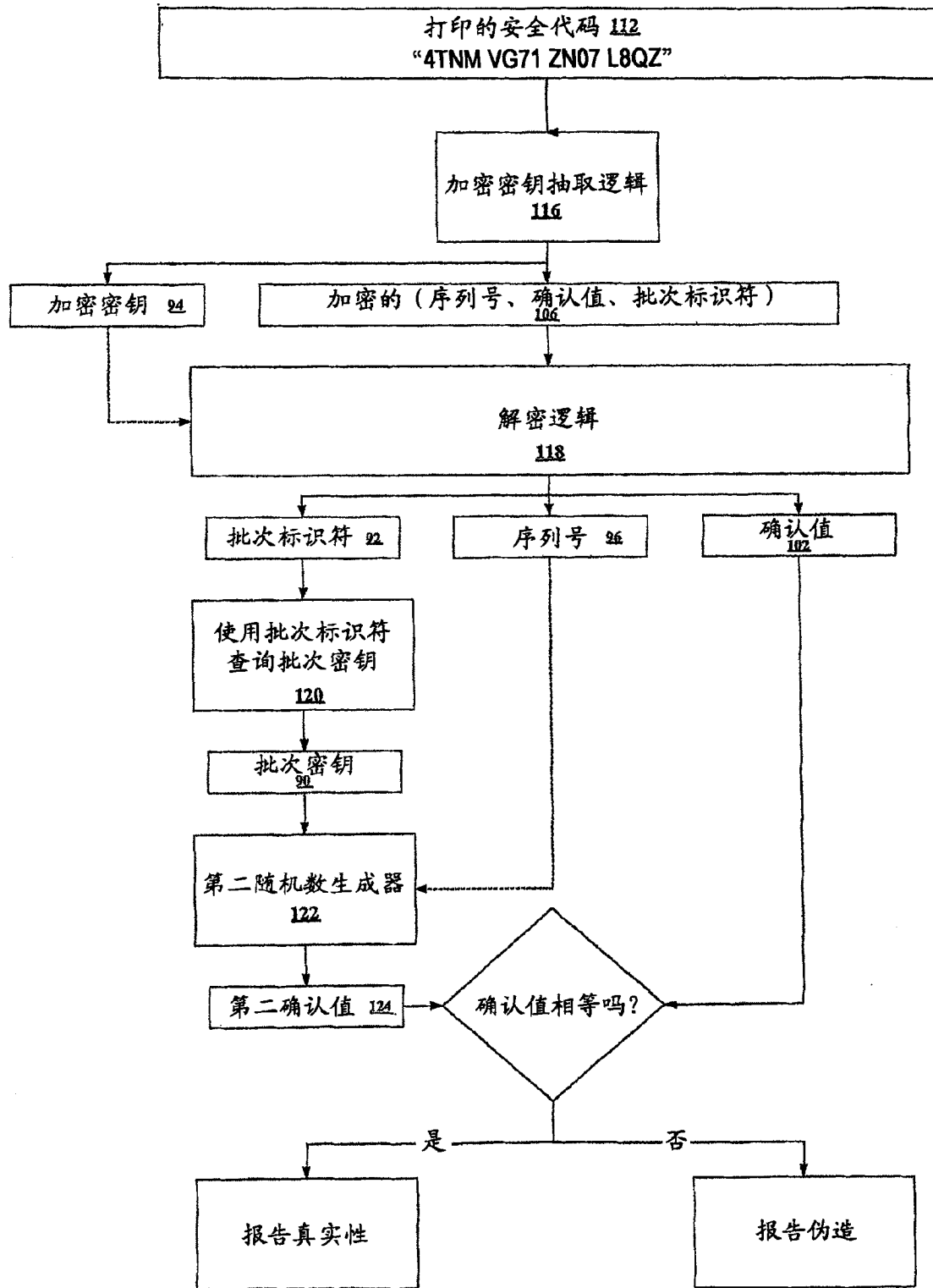


图 5

**130**  
4TNM VG71  
ZN07 L8QZ



图 6A

图 6B

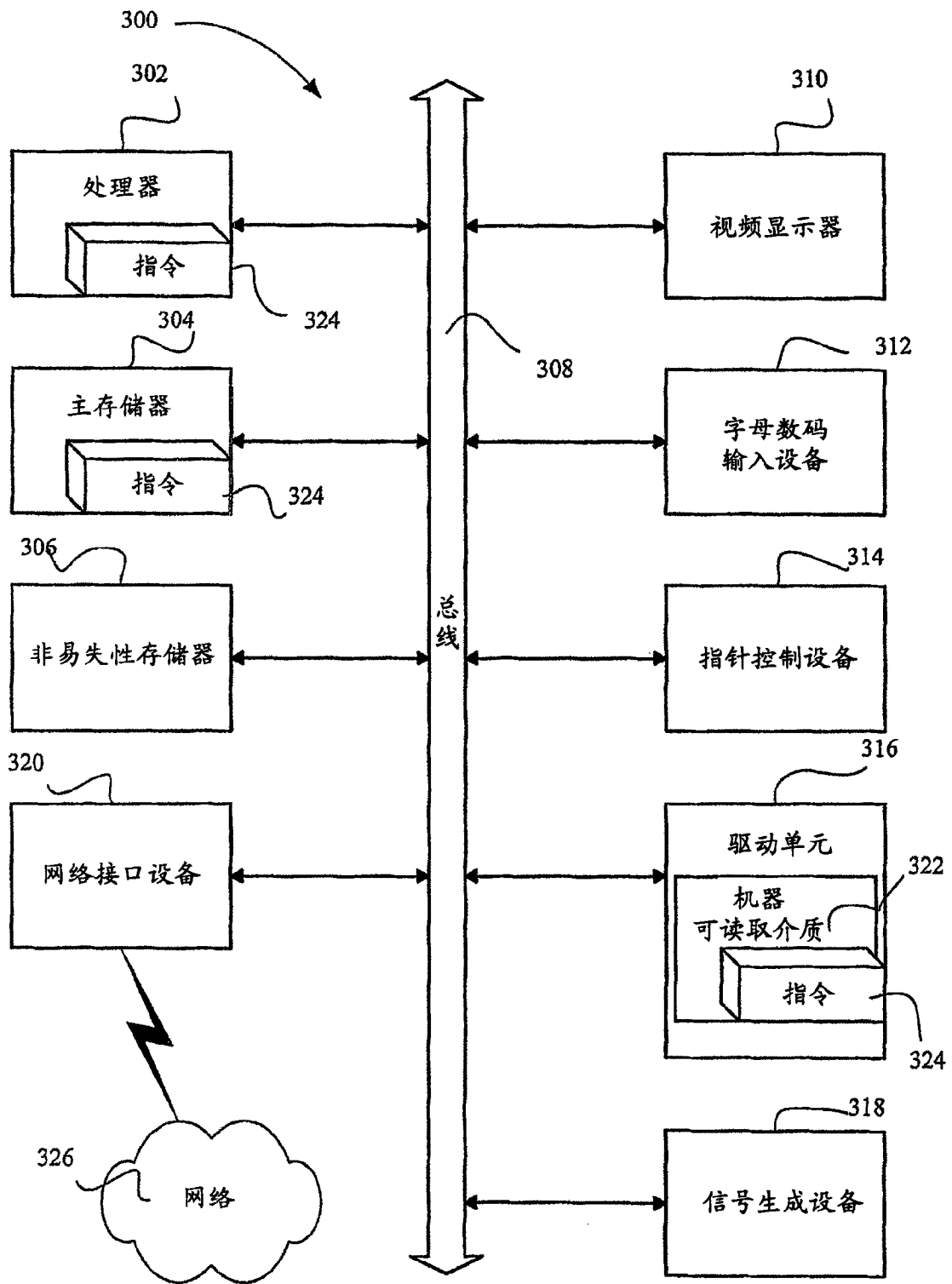


图 7