(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 102103669 B
(45)授权公告日 2015.08.19

(21)申请号 201010603816.5
(22)申请日 2010.12.22
(30)优先权数据
12/645,278 2009.12.22 US
(73)专利权人 英特尔公司
地址 美国加利福尼亚
(72)发明人 D·霍恩德尔
(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 刘瑜 王英
(51)Int.Cl.
G06F 21/31(2013.01)
G06K 7/10(2006.01)
(56)对比文件
CN 1835457 A,2006.09.20,
CN 101529797 A,2009.09.09,
US 20060146071 A1,2006.07.06,
US 2004062399 A1,2004.04.01,
审查员 张桂华

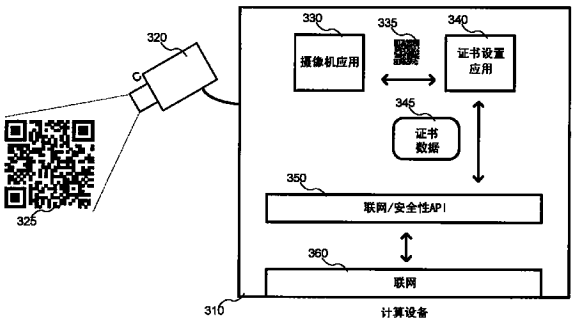
权利要求书3页 说明书10页 附图9页

(54)发明名称

自动安全性控制系统及计算机实现的方法

(57)摘要

描述了用于自动安全性设置的技术和系统的实施例。与计算设备相关联的摄像机可以被用来捕获诸如QR码的多维码的图像。该多维码可以包含用于在计算设备上设置安全性或者联网的信息。例如,所述码可以包含用于将所述计算设备连接到无线网络的信息,或者用于便利安全互连的安全性证书。在捕获图像后,安全性设置应用可以解码包含于所述码中的信息,并且通过操控计算设备上的API来使用其控制计算设备上的安全性和联网。这防止在输入长而难的多条安全性信息时不恰当的连接和/或错误。可以描述和要求保护其他实施例。



CN 102103669 B

1. 一种计算机实现的方法，包括：

在计算设备处，获得多维码的图像；

在所述计算设备处，分析所述多维码以识别编码于其中的一条或多条安全性相关信息，其中，所述多维码包括与对该计算设备进行验证的安全性证书相关的信息并且包括与所述安全性相关信息分离的一个或多个数据单元，所述一个或多个数据单元包括使用意图指示符、版本号、被编码在所述多维码中的数据类型的描述和检错数据；以及

在所述计算设备处，至少部分基于所述安全性相关信息，引导所述计算设备的一个或多个安全性特征的修改，引导所述计算设备的一个或多个安全性特征的修改的操作包括：引导所述计算设备将所述安全性证书提供给网络以用于确定该计算设备被允许在该网络上访问。

2. 如权利要求 1 所述的方法，其中，获得多维码的图像的操作包括：从耦合到所述计算设备的摄像机接收所述多维码的图像。

3. 如权利要求 2 所述的方法，其中，获得多维码的图像的操作还包括：引导耦合到所述计算设备的所述摄像机捕获所述多维码的图像。

4. 如权利要求 2 所述的方法，还包括，在所述计算设备处：

拍摄所述多维码的图像；以及

向用户询问所述多维码中的信息是否应当被用于修改所述一个或多个安全性特征。

5. 如权利要求 1 所述的方法，其中，获得多维码的图像的操作包括：接收二维码的扫描图像。

6. 如权利要求 1-5 之一所述的方法，其中，分析所述多维码的操作包括：从所述数据类型的描述数据单元识别编码于其中的所述安全性相关信息的描述符。

7. 如权利要求 1-5 之一所述的方法，其中，分析所述多维码的操作包括：识别作为编码于其中的多条安全性相关信息的一个或多个加密密钥。

8. 如权利要求 7 所述的方法，其中，分析所述多维码的操作还包括：识别所述一个或多个加密密钥的一个或多个加密类型。

9. 如权利要求 1-5 之一所述的方法，其中，分析所述多维码的操作包括：从所述版本号数据单元识别版本号。

10. 如权利要求 6 所述的方法，其中，当所述描述符表明所述多维码包括与无线网络相关的信息时，引导所述计算设备的一个或多个安全性特征的修改的操作包括：引导所述计算设备使用所述无线网络。

11. 如权利要求 10 所述的方法，其中，分析所述多维码的操作包括：识别所述无线网络的标识符。

12. 如权利要求 6 所述的方法，其中，所述描述符表明所述多维码包括与所述安全性证书相关的信息。

13. 如权利要求 12 所述的方法，其中，分析所述多维码的操作包括：识别所述安全性证书的证书类型。

14. 如权利要求 13 所述的方法，其中，所述安全性相关信息包括与证书机构根证书相关的信息。

15. 如权利要求 6 所述的方法，其中，当所述描述符表明所述多维码包括使用安全性相

关信息来防止对包含于所述多维码中的数据或者对使用包含于所述多维码中的数据传输的其他数据进行未授权访问的信息时，一个或多个安全性特征的修改包括：在涉及包含于所述多维码中的数据的通信期间使用所述安全性相关信息。

16. 一种用于自动安全性控制的系统，包括：

联网接口，其被配置来便利与网络的通信；

耦合到所述联网接口的计算机处理器；

一个或多个联网控制模块，其耦合到所述联网接口，并且被配置来控制所述系统上的联网通信；以及

能够由所述处理器执行的安全性使能模块，所述安全性使能模块被配置来在由所述处理器执行时使得所述系统进行以下操作：

从多维码图像提取安全性修改信息，包括对该系统进行验证的安全性证书被编码在所述多维码中的标识符、在所述证书中使用的加密方法的标识符，以及从二维码图像提取的一个或多个加密密钥；

从所述多维码图像提取与所述安全性修改信息分离的一个或多个数据单元中的数据，所述一个或多个数据单元包括使用意图指示符、版本号、被编码在所述多维码中的数据类型的描述和检错数据；以及

引导所述一个或多个联网控制模块修改对所述系统上联网通信的控制，以在确定该系统被允许在网络访问时使用所述安全性证书。

17. 如权利要求 16 所述的系统，还包括耦合到所述计算机处理器的储存存储器，以及耦合到所述储存存储器的摄像机，其中，所述安全性使能模块还被配置来在由所述计算机处理器执行时将所述摄像机捕获的多维码图像存储在所述储存存储器中。

18. 如权利要求 17 所述的系统，其中，所述安全性使能模块还被配置来在由所述计算机处理器执行时引导所述摄像机捕获多维码图像。

19. 如权利要求 16-18 之一所述的系统，其中：

所述安全性使能模块被配置来在由所述计算机处理器执行时，从所述多维码图像提取无线联网标识符、无线联网安全性协议的标识符以及一个或多个无线联网加密密钥；并且

所述一个或多个联网控制模块包括无线联网修改模块。

20. 如权利要求 16-18 之一所述的系统，其中：

所述一个或多个联网控制模块包括联网加密修改模块。

21. 一种用于自动安全性控制的系统，包括：

用于从耦合到所述系统的摄像机获得二维码的图像的模块；

用于分析所述二维码以识别编码于其中的一条或多条安全性相关信息的模块，其中，所述二维码包括与对该系统进行验证的安全性证书相关的信息并且包括与所述安全性相关信息分离的一个或多个数据单元，所述一个或多个数据单元包括使用意图指示符、版本号、被编码在所述多维码中的数据类型的描述和检错数据；以及

用于至少部分基于所述安全性相关信息，引导所述系统的一个或多个安全性特征的修改的模块，引导所述系统的一个或多个安全性特征的修改的操作包括：引导所述系统在确定该系统被允许在网络上访问时提供所述安全性证书。

22. 如权利要求 21 所述的系统，其中，用于分析所述二维码的模块包括：用于从所述数

据类型的描述数据单元识别编码于其中的所述安全性相关信息的描述符的模块。

23. 如权利要求 22 所述的系统，其中：

所述描述符表明所述二维码包括与无线网络相关的信息，用于引导所述系统的一个或多个安全性特征的修改的模块包括：用于引导所述系统使用所述无线网络的模块；以及

用于分析所述二维码的模块包括：用于识别所述无线网络的标识符的模块。

24. 如权利要求 21-23 之一所述的系统，其中：

用于分析所述二维码的模块包括：识别所述安全性证书的证书类型。

25. 如权利要求 21-23 之一所述的系统，其中，分析所述二维码包括：

用于从所述数据类型的描述数据单元识别作为编码于其中的多条安全性相关信息的一个或多个安全性密钥的模块；

用于从所述数据类型的描述数据单元识别所述一个或多个加密密钥的一个或多个加密类型的模块；以及

用于从所述版本号数据单元识别编码于其中的所述安全性相关信息的版本号的模块。

自动安全性控制系统及计算机实现的方法

技术领域

[0001] 本申请涉及计算机联网和安全性，并且更具体地，涉及提供安全性和联网特征的自动设置。

背景技术

[0002] 很多现有的电子设备，例如膝上型计算机、上网本、PDA 和智能电话，允许用户修改网络和安全性设定。当用户希望改变其联网连接时，例如当面对新的无线网络或者在网络选择间进行切换时，这对于用户来说是有用的。然而，用户可能难以无错误且无阻碍地设置联网。

[0003] 例如，当试图在公共场合使用无线网络时，用户可能必须从多个服务集标识符（也被称为“SSID”）中进行选择，这些 SSID 标识可用的无线网络。如果广播了多个类似命名的 SSID，结果是用户可能会困惑于哪个对他们的使用来说是适当且安全的。在其他的普遍场景中，可用的无线网络可能不会广播其存在，并且因此迫使用户手动输入 SSID。如果该 SSID 是复杂的或者不是传统式拼写的（或者是用户不熟悉的语言），则实际存在用户将错误输入 SSID 的可能性。当此发生时，用户会发现他或她不能连接，或者甚至更糟的是连接到其他非意图的（并且不安全 / 不可信的）、具有类似拼写的 SSID 的无线网络。这对于外行用户来说可能是危险的，他们可能不能意识到他们的连接不当。

[0004] 一些网络使用加密连同密码、密码短语或字符串（例如十六进制键）来防止不当连接。在这种场景下，通常向用户施与对待连接无线网络 SSID 的指示以及响应于提示要键入的密码。不幸的是，该技术提供与上面所讨论的相同的错误输入（密码）的可能性。该问题在密码的情况下更加复杂，因为通常来说密码对于试图键入它们的用户来说不具有内在含义。当密码长且难猜时，用户很可能错误输入，并且即便在检查时也难以纠正错误。当加密要求输入字符串（例如十六进制数字）时可能存在类似的问题。这样的串根据各种加密实现可以包括例如 13 个、26 个或者甚至 52 个字符。因此，用户可能发现他或她为了使用网络而被要求输入诸如“6c736b64666f73766f73696468766f73646968766f7369647633343235”的串。输入这样长的串而不引起错误是困难的。

[0005] 很多这些同样的问题发生在其他安全性和联网环境中，例如 SSL、openVPN 和 openssh。例如，为了与一些安全的网络连接和交互，需要用户使用安全性证书，例如证书机构（“CA”）根证书。在一种场景下，用户将使用证书来验证该用户或该用户的设备被允许在网络上进行访问。在另一场景中，用户将使用与该证书相关联的已知加密密钥来加密消息以进行安全传输。在一些使用情况下，用户可以通过两种不同的手段（例如电子的或纸张印刷的）接收证书拷贝，以确保其被安全地传输。因此，即使当用户接收电子证书时，用户可能仍必须手动输入单独接收的证书信息，以便于核实该证书是有效的。

[0006] 但是，由于安全性证书利用了加密，该手动输入可能存在类似于无线联网所存在的问题。加密密钥，尤其是在安全性证书中使用的那些，可能长达数百甚至上千字符。期望用户正确地输入如此大量的数据通常是不实际的，尤其是当这些数据对于用户来说没有明

显的结构(例如在加密密钥或加密的证书数据中)时更是如此。一些系统可能试图通过拍摄证书打印版本的图像并使用光学字符识别以提取信息来减轻该问题。然而,即便使用这些技术,数据的众多以及光学字符识别的不精确性意味着很可能引入不期望的错误。

发明内容

[0007] 根据本发明的一个方面,提供一种计算机实现的方法,包括:在计算设备处,获得多维码的图像;在所述计算设备处,分析所述多维码以识别编码于其中的一条或多条安全性相关信息,其中,所述多维码包括与对该计算设备进行验证的安全性证书相关的信息;以及在所述计算设备处,至少部分基于所述安全性相关信息,引导所述计算设备的一个或多个安全性特征的修改,引导所述计算设备的一个或多个安全性特征的修改的操作包括:引导所述计算设备将所述安全性证书提供给网络以用于确定该计算设备被允许在该网络上访问。

[0008] 根据本发明的另一个方面,提供一种用于自动安全性控制的系统,包括:联网接口,其被配置来便利与网络的通信;耦合到所述联网接口的计算机处理器;一个或多个联网控制模块,其耦合到所述联网接口,并且被配置来控制所述系统上的联网通信;以及能够由所述处理器执行的安全性使能模块,所述安全性使能模块被配置来在由所述处理器执行时使得所述系统进行以下操作:

[0009] 从多维码图像提取安全性修改信息,包括对该系统进行验证的安全性证书被编码在所述多维码中的标识符、在所述证书中使用的加密方法的标识符,以及从二维码图像提取的一个或多个加密密钥;以及引导所述一个或多个联网控制模块修改对所述系统上联网通信的控制,以在确定该系统被允许在网络上访问时使用所述安全性证书。

[0010] 根据本发明的再一个方面,提供一种用于自动安全性控制的系统,包括:用于从耦合到所述系统的摄像机获得二维码的图像的模块;用于分析所述二维码以识别编码于其中的一条或多条安全性相关信息的模块,其中,所述二维码包括与对该系统进行验证的安全性证书相关的信息;以及用于至少部分基于所述安全性相关信息,引导所述系统的一个或多个安全性特征的修改的模块,引导所述系统的一个或多个安全性特征的修改的操作包括:引导所述系统在确定该系统被允许在网络上访问时提供所述安全性证书。

附图说明

[0011] 将通过示例性实施例而非限制的方式描述本发明的实施例,所述示例性实施例在附图中图示,在附图中,类似的标号指代类似的部件,并且在附图中:

[0012] 图 1 是图示根据本公开各个实施例的使用实例的图;

[0013] 图 2 是图示根据各个实施例的组件的一个实例的框图;

[0014] 图 3 是图示根据各个实施例的组件的另一个实施例的框图;

[0015] 图 4 是根据各个实施例的编码的安全性信息的实例;

[0016] 图 5a 和 5b 是根据各个实施例的示例性类型的编码的安全性信息;

[0017] 图 6 图示根据各个实施例的示例性安全性信息获取过程;

[0018] 图 7 图示根据各个实施例的另一示例性安全性信息获取过程;

[0019] 图 8 图示根据各个实施例的示例性安全性设置过程;以及

[0020] 图 9 图示根据各个实施例的示例性计算环境。

具体实施方式

[0021] 本发明的说明性实施例包括但不限于使用通过非原发性(non-primary)输入方法输入安全性信息(例如通过扫描多维码以提取其中编码的安全性信息)来进行自动安全性设置的方法和装置。该技术可以使用运行于一设备上的专用应用或计算机进程,所述设备从对多维码拍摄的图像提取安全性信息并且引导该设备设置一个或多个安全性特征。可以设置的安全性特征的实例可以包括到无线网络的连接或特定安全性证书的使用。通过在相对致密的多维码中提供信息,希望提供与用户的安全交互的实体可以容易地提供连接或安全性信息,同时降低信息被错误输入的可能性。

[0022] 将使用本领域技术人员向本领域其他技术人员传达他们的工作内容时通常所使用的术语来描述说明性实施例的各个方面。然而,对于本领域的技术人员来说将显而易见的是,可以仅利用所描述的方面中的一些来实施替换性实施例。为了解释说明的目的,阐述了特定的数字、材料和配置以提供对说明性实施例的全面理解。然而,对于本领域技术人员来说将显而易见的是,可以在没有这些特定细节的情况下实施替换实施例。在其他实例中,公知特征将被省略或简化,以免模糊这些说明性实施例。

[0023] 此外,以最有助于理解说明性实施例的方式将各种操作依次描述为多个分离的操作 ;然而,描述的顺序不应当被解释为暗示这些操作必定是顺序相关的。特别地,这些操作不需按照表述的顺序来执行。

[0024] 短语“在一个实施例中”或“在实施例中”被重复地使用。这个短语通常不表示相同的实施例 ;然而,也可以表示相同的实施例。术语“包含”、“具有”、“包括”是同义词,除非上下文另有规定。短语“A/B”表示“A 或 B”。短语“A 和 / 或 B”表示“(A),(B),或 (A 和 B)”。短语“A,B 和 C 中至少一个”表示“(A),(B),(C),(A 和 B),(A 和 C),(B 和 C) 或 (A,B 和 C)”。

[0025] 如上面讨论的,本技术和系统的实施例包括无线设置应用,所述无线设置应用可以通过使用诸如二维 QR 码的多维码来便利无线网络的设置。在例如通过捕获码图像而将 QR 码导入到设备中之后,该应用可以提取可以被编码在所述 QR 码中的结构化信息。该信息随后可以引导所述应用来设置所述设备使用特定无线网络。另外,如果无线网络要求特定设定,例如包括使用密码或密码短语,则所述应用可以包括对这些信息的设置。在各个实施例中,可以通过使用已知的 API 来进行无线网络的设置,所述 API 是由所述设备上的安全性和联网服务提供的,例如操作系统提供的 API。

[0026] 本技术和系统的实施例还可以包括安全性证书设置应用,所述安全性证书设置应用可以便利安全性证书(例如根证书)的设置和使用。在各个实施例中,证书信息可以被编码在诸如二维 QR 码的多维码中。在扫描了码的图像之后,所述证书信息可以被提取并用于未来需要安全性和信任的通信中。可替换地,在各个实施例中,所述应用可以使用编码的经打印的证书信息来核实已经接收的、设备已知的安全性证书。

[0027] 尽管本文讨论的技术和装置是参照“安全性”的设置来讨论的,但是该术语可以被理解为包括各种形式的安全性和联网,所述安全性和联网将额外信息(尤其是长和 / 或难于输入的信息)用于其设置。例如,在各个实施例中,“安全性”可以包括联网、无线联网、加

密和安全性证书，以及其他形式的数据。这些数据可能是以难于输入的形式提供的，或者是以对于传送到安全性相关联系统来说困难或者复杂的其他形式提供的。另外，在各个实施例中，安全性相关信息可以不是用于设置、修改或维护安全性协议的信息，而相反可以是用于其他目的的安全信息。因此，安全性信息可以包括这样的数据，其使用安全性相关技术来防止对数据本身或传输的其他数据的未授权读取、解译、篡改或修改，所述传输的其他数据使用包含于安全性信息中的数据来实现与该信息相关联的目标。例如，除了上述安全性相关信息的描述之外，这样的信息可以包括与在线支付相关的编码的信息。

[0028] 图 1 图示本公开的自动无线设置技术的各个实施例。如上面讨论的，在各个实施例中，可以使得无线网络 110 可用。为了提供对该无线网络的访问，在各个实施例中，在图 1 中被图示为二维 QR 码的多维码 120 可以与该无线网络相关联。在各个实施例中，由无线网络 110 的提供商借由使用对多维码 120 的公众可视显示来使该关联为可获得的。在各个实施例中，该多维码可以显示为打印在诸如纸张、塑料或金属的物理材料上，或者可以显示在电子显示器上。

[0029] 尽管出于图示的目的而使用了显示 URL 的 QR 码，但是在各个实施例中该多维码 120 可以显示不同的或者更复杂或不那么复杂的信息，包括格式化的信息。例如，XML 码可以被编码到多维码 120 中。另外，在各个实施例中，在编码于多维码中的信息内可以包括元数据，所述元数据包括但不限于对其中编码的数据的描述、版本号和 / 或纠错校验和（未图示）。在各个实施例中，多维码也可以采取其他形式，而不仅限于使用 QR 码。

[0030] 如图 1 所图示的，根据各个实施例，可以采用耦合到摄像机 130 的电子设备 140。在各个实施例中，设备 140 可以包括各种大小、能力、形状因子的计算设备，包括但不限于膝上型计算机、笔记本计算机和桌面型计算机、上网本、PDA 和智能电话。另外，尽管所图示的实施例将摄像机 130 图示为与计算设备 140 分离的实体，但是在各个实施例中，摄像机可以集成在计算设备 140 中。因此，在一个实例中，计算设备 140 可以包括本身即包含内部摄像机的智能电话。在可替换的实施例（未图示）中，可以使用扫描仪或其他图像接收设备取代摄像机 130 来获取码图像。

[0031] 尽管在图示的实施例中计算设备 140 将包括一个或多个联网能力（capability），包括用于无线联网的卡或其他设备，但是在各个实施例中，计算设备 140 可以不包括这些能力，并且可以针对在无线网络之外设置安全性或其他服务而使用本技术的各种实施例。

[0032] 如图 1 所图示以及早前所暗指的，本技术的实施例可以被用于设置无线网络。因此，设备 140 的摄像机 130 可以用于捕获与无线网络 110 相关联的多维码 120 的图像。在该图像捕获之后，可以通过使用该设备上的设置应用以及所提取的信息而被处理，以设置所述计算设备 140 来使用无线网络 110。如图 1 下半部所图示的，在该设置之后，计算设备 140 可以随后与无线网络 110 交互并且在无线网络 110 上通信。

[0033] 图 2 图示根据各个实施例可以在计算设备内用来便利无线网络的设置的组件和数据流的框图。如图所示并且如上面讨论的，各个实施例包括摄像机 220（在各个实施例中，该摄像机 220 可以包括图 1 所图示的摄像机 130），该摄像机 220 可以拍摄诸如所图示 QR 码 225 的多维码的图像。该摄像机可以耦合到计算设备 210，在各个实施例中计算设备 210 可以包括图 1 所图示的计算设备 140。类似于关于图 1 所进行的讨论，尽管图 2 图示出在计算设备 210 外部的摄像机 220，但是在各个实施例中摄像机 220 可以整体或部分在计算

设备 210 内部。

[0034] 本技术的各个实施例是与计算设备 210 上操作的应用和服务相关地进行的。例如，所图示的计算设备 210 可以包括摄像机应用 230。该摄像机应用 230 可以被用于引导摄像机 220 的操作。因此，当用户期望捕获多维码 225 的图像时，用户可以引导摄像机应用来促使摄像机获取码图像 235。在各个实施例中，该码图像 235 随后可以被无线设置应用 240 共享或者传送到无线设置应用 240。

[0035] 在各个实施例中，无线设置应用 240 本身可以引导摄像机应用 230 来捕获图像。在各种可替换实施例中，摄像机应用 230 可以在没有无线设置应用 240 的引导的情况下捕获多维码 225 的图像 235。在一些这样的实施例中，摄像机应用可以在捕获图像之后请求来自用户的关于无线设置应用是否应当启动并用来解码多维码 225 中包含的信息的引导。在各个实施例中，摄像机应用 230 自身可以具备解码多维码 225 的某种能力。在各个实施例中，该多维码 225 中的信息可以引导摄像机应用启动无线设置应用或者以其他方式与无线设置应用进行通信。另外，在各个实施例中，无线设置应用可以包括独立应用、独立进程和 / 或作为一个或多个其他应用或进程的从属而执行的一个或多个子例程或库。

[0036] 无线设置应用 240 随后可以使用编码在图像 235 中的信息（被图示为无线设置数据 245）来控制一个或多个无线联网 API250。这些 API250 继而可以控制无线联网服务 260 来根据所述无线设置数据 245 为计算设备 210 提供无线联网能力。

[0037] 图 3 图示根据各个实施例可以在计算设备内用来实现使用安全性证书进行安全通信的组件和数据流的框图。如图所示并且如上面讨论的，各个实施例包括摄像机 320（在各个实施例中，该摄像机 320 可以包括图 1 所图示的摄像机 130 和 / 或图 2 所图示的摄像机 220），该摄像机 320 可以拍摄诸如所图示 QR 码 325 的多维码的图像。该摄像机可以耦合到计算设备 310，在各个实施例中该计算设备 310 可以包括图 1 所图示的计算设备 140。类似于上面讨论的，尽管图 3 图示出在计算设备 310 外部的摄像机 320，但是在各个实施例中摄像机 320 可以整体或部分在计算设备 310 内部。

[0038] 本技术的各个实施例是与计算设备 310 上操作的应用和服务相关地进行的。例如，所图示的计算设备 310 可以包括摄像机应用 330。该摄像机应用 330 可以被用于引导摄像机 320 的操作。因此，当用户期望捕获多维码 325 的图像时，用户可以引导摄像机应用来促使摄像机获取码图像 335。在各个实施例中，该码图像 335 随后可以被证书设置应用 340 共享或者传送到证书设置应用 340。

[0039] 在各个实施例中，证书设置应用 340 本身可以引导摄像机应用 330 捕获图像。在各种可替换实施例中，摄像机应用 330 可以在没有证书设置应用 340 的引导的情况下捕获多维码 325 的图像 335。在一些这样的实施例中，摄像机应用可以在捕获图像之后请求来自用户的关于无线设置应用是否应当启动并用来解码多维码 325 中包含的信息的引导。在各个实施例中，摄像机应用 330 自身可以具备解码多维码 325 的某种能力。在各个实施例中，该多维码 325 中的信息可以引导摄像机应用启动证书设置应用或者以其他方式与证书设置应用进行通信。另外，在各个实施例中，证书设置应用可以包括独立应用、独立进程和 / 或作为一个或多个其他应用或进程的从属而执行的一个或多个子例程或库。

[0040] 证书设置应用 340 随后可以使用编码在图像 335 中的信息（在图 3 中被图示为证书数据 345）来控制一个或多个联网 / 安全性 API350。这些 API350 继而可以控制联网服务

360 来使用证书数据 345 为计算设备 310 提供联网能力。

[0041] 图 4 图示根据各个实施例可以编码在多维码中的数据单元(data element)的一般结构的实例。图 4 中所图示的数据类型可以与本文所描述的无线网络设置和安全性证书设置技术两者一起使用。在各个实施例中,所图示的数据单元可以被组合、分割或省略。在各个实施例中,图 4 所图示的数据单元可以由本文描述实施例的一个或多个组件或处理来解码或解释。

[0042] 首先图示的数据单元是使用意图指示单元 412。在各个实施例中,该指示可以包括指示数据当前被编码在多维码中的目的的码或其他数据。例如,图 2 中所图示的二维 QR 码 225 可以包含单元 412 处指示该码要被用于设置无线网络的信息。相反,在图 3 图示的实施例中,使用意图指示单元 412 可以指示二维 QR 码 325 包含安全性证书信息。

[0043] 接下来,图 4 图示版本号单元 414。在各个实施例中,版本号单元 414 被编码来为编码于多维码中的信息结构提供版本控制(versioning)支持。在各个实施例中,设置应用可以维护关于编码的安全性信息的不同版本的知识。不同的版本可以包括不同信息或者可以以不同方式结构化 ;通过提供版本号,设置应用能够预测何种类型的信息被编码在多维码中,并且相应地解译该码。例如,多维码中的信息可以包括致密的或可能压缩的数据块,设置应用可以单独或部分基于版本号单元 414 所指示的预先协定的结构来解码和解译所述数据块。因此,在一个实例中,设置应用可以根据版本号知道遵从(up to)具体转义码的字符包括 SSID,其后紧跟加密类型的指示,然后是根据加密类型所确定的内容(例如在后续字节中用于 WEP 加密的加密密钥、与之相对的关于验证协议的信息,其后跟随着验证数据、加密协议以及用于 WPA2 加密的加密数据)。在这样的场景下,XML 或其他自描述数据格式不可以用于对数据进行结构化。使用版本号可以加速对码的解码,并且还允许公布这些码的实体随时间而演进编码的信息的结构。

[0044] 接下来,可以包括数据类型描述单元 416。在各个实施例中,该描述可以包括被编码在多维码本身中的数据类型的列表。在其他实施例中,该数据类型描述可以是对另一文档或规范的引用,所述文档或规范本身描述了一组数据类型。在各个实施例中,数据类型描述可以与版本号单元 414 组合。

[0045] 接下来,图示了安全性 / 联网数据单元 418。在各个实施例中,数据类型描述单元 416 和安全性 / 联网数据单元 418 可以组合成自描述性的单个单元或分层结构。例如,数据可以以 XML 码的形式编码,该 XML 码如同其呈递数据那样来描述数据。接下来,图示了检错数据单元 420。该单元可以被用于帮助核实从多维码所解码的数据的正确性。在各个实施例中,检错码可以被实现为校验和或更复杂的检错数据。在各个实施例中,检错数据可以替代于或者附加于校验和或者在多维码规范中提供并在编码和显示多维码时创建的其他检错数据而存在。

[0046] 图 5a 和 5b 图示根据各个使用实施例可以被编码在多维码中的数据单元的结构的示例性实现。例如,图 5a 所图示的数据结构可以与无线网络设置实施例(例如图 2 所示的实施例)一起使用,而图 5b 所图示的数据结构可以与安全性证书设置实施例(例如图 3 所图示实施例)一起使用。在各个实施例中,图 5a 和 5b 图示的数据单元可以被组合、分割或部分省略。在各个实施例中,图 5a 和 5b 所图示的数据单元可以由本文所描述实施例的一个或多个组件或处理来解码或解译。

[0047] 图 5a 以图示数据单元 532 开始，该数据单元 532 指示数据被用于无线设置。该数据单元 532 之后可以跟随着数据单元 534，该数据单元 534 说明无线设置版本号。在各个实施例中，并且如图 5a 所图示的，其中编码的版本号可以基于与针对不同使用意图的版本号不同的编号系统；可替换地，可以跨多种用途使用一个版本编号系统，从而该版本号整体或部分标识编码的信息的使用意图。如上面讨论的，在各个实施例中，版本号可以指示针对其他数据预先协定的结构，而不是使用自描述数据或者包括在多维码内包含的描述。

[0048] 接下来，图 5a 图示了数据单元 536，该数据单元 536 指示被编码在多维码中的数据类型。例如并且如随后在数据单元 538、540、542 和 544 中说明的，数据类型单元 536 可以指示该多维码包括关于以下项的信息：无线网络 SSID、该无线网络上所用加密和 / 或协议的类型、可以用于获得对该网络的访问的加密密钥或密码短语，以及可以用来连接的其他网络参数（例如信道或代理信息）。在该数据描述之后，多维码包括被图示为数据单元 538、540、542 和 544 的 SSID、加密 / 协议类型、密钥 / 密码短语以及其他参数数据单元本身。另外，图 5a 图示出该多维码包括如上所述的校验和单元 546，以允许解码处理检查所包括数据的有效性。

[0049] 图 5b 以图示数据单元 562 开始，该数据单元 562 指示数据要用于证书设置。这之后跟随着说明证书设置版本号的数据单元 564。如上面参照图 5a 讨论的，在各个实施例中并且如图 5b 图示的，其中编码的版本号可以基于与针对不同使用意图的版本号不同的编号系统；可替换地，可以跨多种用途使用一个版本编号系统，从而该版本号整体或部分标识所编码信息的使用意图。

[0050] 接下来，图 5b 图示了数据单元 566 和 568，它们指示可以被编码在多维码中的证书类型和加密类型。在该数据描述之后，多维码可以包括被图示为数据单元 570 和 572 的证书数据和加密密钥数据。最后，图 5b 图示出该多维码可以包括如上所述的校验和单元 574，以允许解码处理检查所包括数据的有效性。

[0051] 图 6 图示根据各个实施例的用于使用编码于多维码中的信息来按照安全性设置应用的引导为计算设备进行自动安全性设置的示例性过程 600。如图示的，在各个实施例中，图 6 所图示的框中所进行的处理可以被组合或者进一步分割为子处理，并且可以重排序。尽管图 6 所图示的动作是参照“安全性”的设置来讨论的，但是该术语可以被理解为包括各种形式的安全性和联网，所述安全性和联网将额外信息（尤其是长和 / 或难于输入的信息）用于其设置。例如，在各个实施例中，“安全性”可以包括联网、无线联网、加密和安全性证书。

[0052] 处理在框 610 开始，在此用户或计算机可以起动安全性应用。在各个实施例中，用户可以通过引导应用执行来起动所述应用；或者，应用可以在起动时自动执行或与摄像机或其他设备的激活相关联地执行。接下来，在框 620，用户可以开启摄像机以允许将多维码输入到系统中。在各个实施例中，摄像机可以与计算设备相关联，例如并入到计算设备中或者以其他方式附接到计算设备。

[0053] 所图示的处理随后可以前进到在框 630 处拍摄多维码的图像。如上面讨论的，根据各个实施例，可以在安全性设置应用的引导下拍摄该图像。接下来，在框 640，安全性设置应用可以解码所述码并且使用其中编码的信息来进行安全性设置，例如设置设备以在无线网络上进行交互，或者在联网通信中使用安全性证书。

[0054] 图 7 图示根据各个实施例用于使用编码于多维码中的信息来为使用安全性设置应用的计算设备进行自动安全性设置的示例性过程 700。在各个实施例中，可以在没有安全性设置应用的引导的情况下进行作为图 7 所示处理的一部分进行的动作。相反，图 7 所示过程是可以如何使用非安全性设置专用应用进行自动安全性设置中某些动作的实例。

[0055] 如图示的，在各个实施例中，图 7 所图示的框中所进行的处理可以被组合或者进一步分割为子处理，并且可以重排序。尽管图 7 所图示的动作是参照“安全性”的设置来讨论的，但是该术语可以被理解为包括各种形式的安全性和联网，所述安全性和联网将额外信息（尤其是长和 / 或难于输入的信息）用于其设置。例如，在各个实施例中，“安全性”可以包括联网、无线联网、加密和安全性证书。这些数据可能是以难于输入的形式提供的，或者是以对于传送到安全性相关联系统来说困难或者复杂的其他形式提供的。另外，在各个实施例中，安全性相关信息可以不是用于设置、修改或维护安全性协议的信息，而相反可以是用于其他目的的安全信息。因此，安全性信息可以包括这样的数据，其使用安全性相关技术来防止对数据本身或传输的其他数据的未授权读取、解译、篡改或修改，所述传输的其他数据使用包含于安全性信息中的数据来实现与该信息相关联的目标。例如，除了上述安全性相关信息的描述之外，这样的信息可以包括与在线支付相关的编码的信息。

[0056] 该处理开始于框 710，在此用户或计算机可以开启摄像机以捕获多维码的图像。在各个实施例中，摄像机可以与计算设备相关联，例如并入到计算设备中或者以其他方式附接到计算设备。接下来，在框 720，在各个实施例中用户可以使用摄像机应用引导摄像机捕获多维码的图像。接下来，在框 730，可以解码所述码。在各个实施例中，该解码可以由摄像机应用在没有来自安全性设置应用的输入的情况下进行。在可替换的实施例中，可以采用多维码读取应用（例如 QR 码读取器应用）来在利用安全性设置应用之前解码多维码中的一些或全部信息。

[0057] 接下来，在框 740，解码了多维码的应用可以确定要通过该码来便利安全性设置。在一个实施例中，这可以通过识别位于多维码内的使用意图标识符或者指向自动安全性设置应用的应用标识符来实现。在一些实施例中，这可以通过标识出设置信息被包括的 URL 或其他信息连同计算设备上的映射的使用来实现，所述映射使得要执行自动安全性设置应用来处理该信息。在各个实施例中，在框 750，计算设备随后可以从用户请求启动安全性设置应用的许可，以便于继续修改或设置各种安全性特征。如果请求并给予了这样的许可，则随后该处理可以继续到框 760，在此启动安全性设置应用，并向其传递编码的信息以进行处理。在各个实施例中，所传递的信息可以仍旧为多维图像的形式，或者可以被完全或部分解码，以由安全性设置应用进行处理。

[0058] 图 8 图示安全性设置应用使用编码于多维码中的信息来进行自动安全性设置的示例性过程 800。在各个实施例中，可以在根据例如上面参照图 6 和 7 描述的处理从多维码获取信息之后进行图 8 的处理。如图示的，在各个实施例中，图 8 所图示的框中所进行的处理可以被组合或者进一步分割为子处理，并且可以重排序。尽管图 8 所图示的动作是参照“安全性”的设置来讨论的，但是该术语可以被理解为包括各种形式的安全性和联网，所述安全性和联网将额外信息（尤其是长和 / 或难于输入的信息）用于其设置。例如，在各个实施例中，“安全性”可以包括联网、无线联网、加密和安全性证书。这些数据可能是以难于输入的形式提供的，或者是以对于传送到安全性相关联系统来说困难或者复杂的其他形

式提供的。另外，在各个实施例中，安全性相关信息可以不是用于设置、修改或维护安全性协议的信息，而相反可以是用于其他目的的安全信息。因此，安全性信息可以包括这样的数据，其使用安全性相关技术来防止对数据本身或传输的其他数据的未授权读取、解译、篡改或修改，所述传输的其他数据使用包含于安全性信息中的数据来实现与该信息相关联的目标。例如，除了上述安全性相关信息的描述之外，这样的信息可以包括与在线支付相关的编码的信息。

[0059] 该处理开始于框 810，在此安全性设置应用可以提取码的使用意图的指示符。接下来，在框 820，安全性设置应用可以提取码的版本号，随后在框 830 提取码中所包含的数据描述。在各个实施例中，使用在框 810-830 所提取的信息，安全性设置应用可以确定包含于码中的信息为何种结构，并且可以知道多维码实际数据有效载荷将应用什么参数和设定，以及可以用来控制计算设备进行所期望安全性设置的 API。接下来，在框 840，安全性设置应用可以提取针对数据类型的数据值，所述数据类型是早前在框 810-830 的处理之后确定的。另外，在框 840，安全性设置应用可以使用提取的数据值以及在之前动作中所获得的关于其含义的知识来操作联网和 / 或安全性 API。例如，安全性设置应用可以修改一个或多个安全性特征所使用的值，或者为这些特征提供新的值；可替换地，可以开启或关闭或者可以停止或开始安全性特征、协议或处理。在使用这些 API 进行设置之后，该过程可以结束。

[0060] 本文描述的技术和装置可以被实现为使用适当硬件和 / 或软件来按需配置的系统。图 9 说明了一个实施例的示例性系统 900，其包括一个或多个处理器 904、耦合到一个或多个处理器 904 中的至少一个的系统控制逻辑 908、耦合到系统控制逻辑 908 的系统存储器 912、耦合到系统控制逻辑 908 的非易失性存储器（NVM）/ 储存器 916，以及耦合到系统控制逻辑 908 的一个或多个通信接口 920。

[0061] 一个实施例的系统控制逻辑 908 可以包括任何适当的接口控制器，用于提供到一个或多个处理器 904 中的至少一个的任何适当的接口，和 / 或到与系统控制逻辑 908 通信的任何适当设备或组件的任何适当的接口。

[0062] 一个实施例的系统控制逻辑 908 可以包括一个或多个存储器控制器，用于提供与系统存储器 912 的接口。系统存储器 912 可以用于加载和存储例如用于系统 900 的数据和 / 或指令。一个实施例的系统存储器 912 可以包括任何适当的易失性存储器，例如，适当的动态随机存取存储器（DRAM）。

[0063] 一个实施例的系统控制逻辑 908 可以包括一个或多个输入 / 输出（I/O）控制器，用于提供与 NVM/ 储存器 916 和通信接口 920 的接口。

[0064] NVM/ 储存器 916 可以用于例如存储数据和 / 或指令。NVM/ 储存器 916 可以包括诸如闪速存储器这样的任何适当的非易失性存储器，和 / 或可以包括任何适当的非易失性存储设备，例如，一个或多个硬盘驱动器（HDD）、一个或多个固态驱动器、一个或多个光盘（CD）驱动器，和 / 或一个或多个数字通用盘（DVD）驱动器。

[0065] NVM/ 储存器 916 可以包括如下所述的存储资源：其在物理上是系统 900 所安装到的设备的一部分，或者其可以被该设备访问，而并不一定是该设备的一部分。例如，NVM/ 储存器 916 可以经由通信接口 920 通过网络被访问。

[0066] 系统存储器 912 和 NVM/ 储存器 916 具体可以分别包括安全性设置逻辑 924 的临时拷贝和永久拷贝。安全性设置逻辑 924 可以包括指令，所述指令在被一个或多个处理器

904 中的至少一个处理器执行时使得系统 900 进行例如结合本文所述无线设置或证书设置应用所描述的自动安全性设置动作。在一些实施例中，安全性设置逻辑 924 可以附加地 / 可替换地位于系统控制逻辑 908 中。

[0067] 通信接口 920 可以为系统 900 提供接口，以通过一个或多个网络和 / 或与任何其它适当设备进行通信。通信接口 920 可以包括任何适当的硬件和 / 或固件。一个实施例的通信接口 920 可包括例如网络适配器、无线网络适配器、电话调制解调器和 / 或无线调制解调器。对于无线通信，一个实施例的通信接口 920 可以使用一个或多个天线。

[0068] 对于一个实施例，一个或多个处理器 904 中的至少一个可以与系统控制逻辑 908 的一个或多个控制器的逻辑封装在一起。对于一个实施例，一个或多个处理器 904 中的至少一个处理器可以与系统控制逻辑 908 的一个或多个控制器的逻辑封装在一起，以形成封装内系统（SiP）。对于一个实施例，一个或多个处理器 904 中的至少一个处理器可以与系统控制逻辑 908 的一个或多个控制器的逻辑集成在同一个硅核上。对于一个实施例，一个或多个处理器 904 中的至少一个处理器可以与系统控制逻辑 908 的一个或多个控制器的逻辑集成在同一个硅核上，以形成片上系统（SoC）。

[0069] 在各实施例中，系统 900 可以具有更多或更少的组件和 / 或不同的架构。

[0070] 尽管本文已经说明和描述了特定实施例，但是本领域技术人员将意识到，在不偏离本发明的实施例的范围的情况下，广泛的各种替代实现和 / 或等价实现可以替换所示出和描述的特定实施例。本申请意图覆盖本文所讨论的实施例的任何修改或变型。因此，显而易见的意思是，本发明的实施例仅受所附权利要求及其等价物的限制。

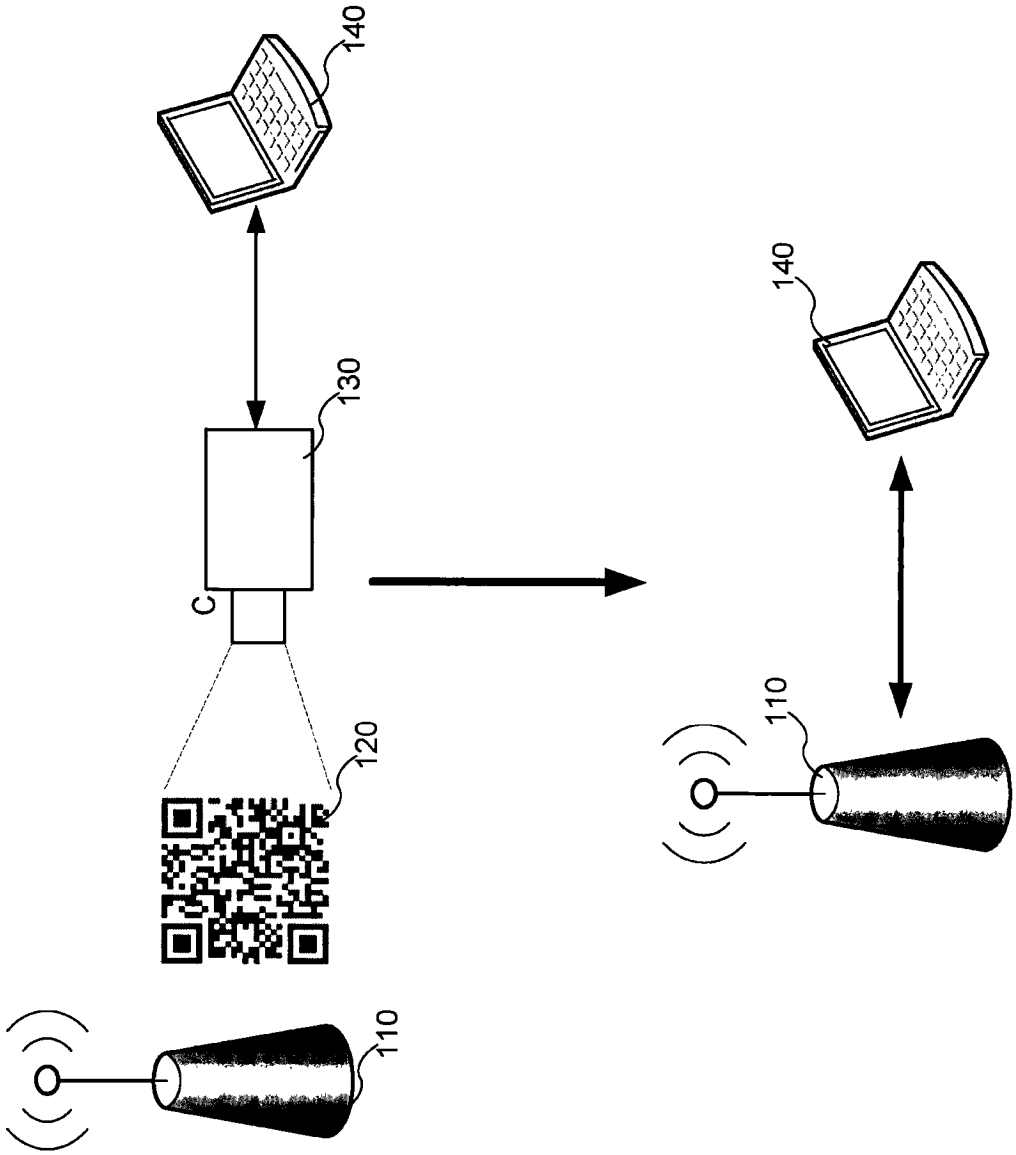


图 1

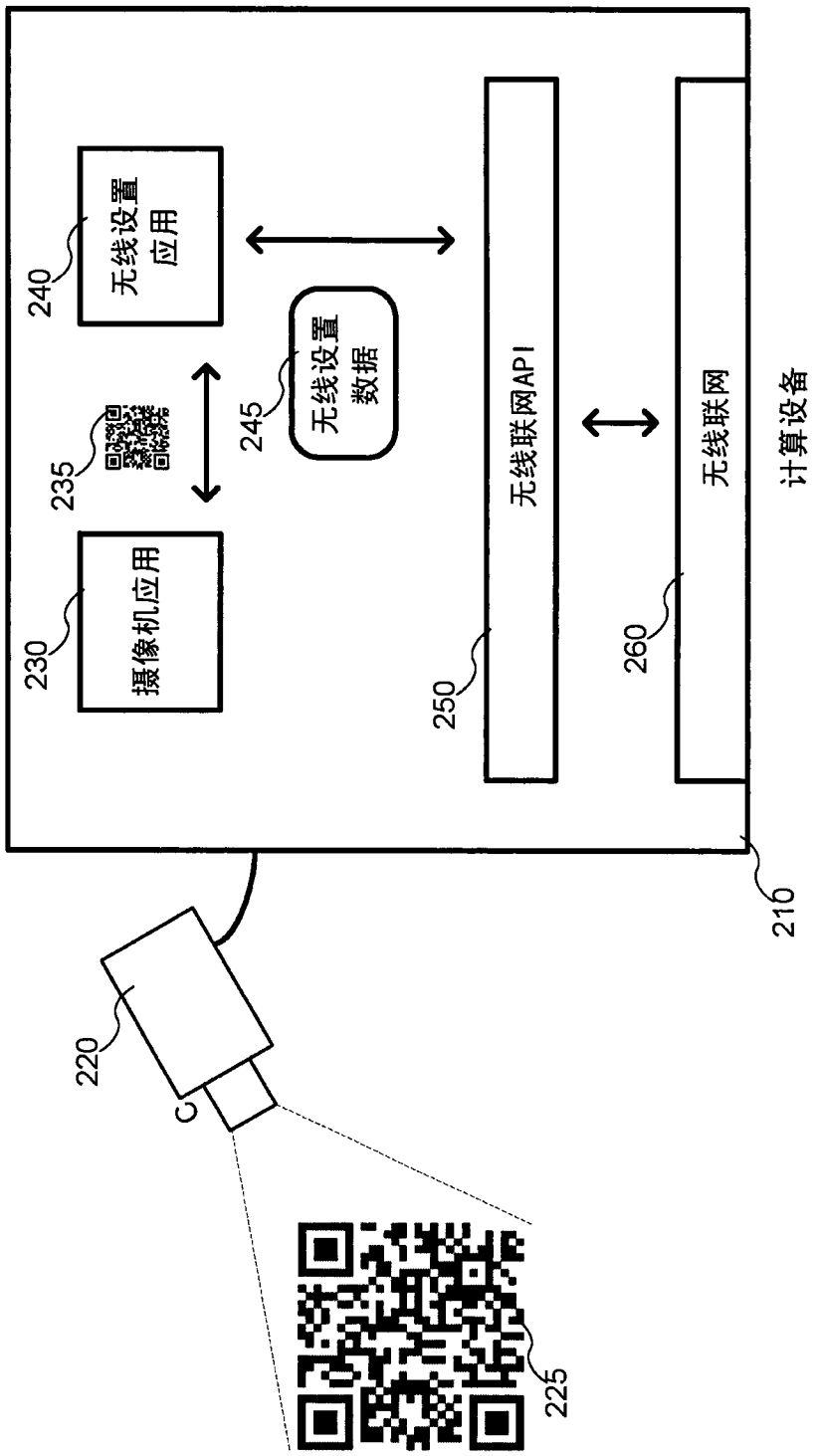

240
无线设置应用
245
无线设置数据
235
230
摄像机应用
250
无线联网API
260
无线联网
计算设备
210
220
225

图 2

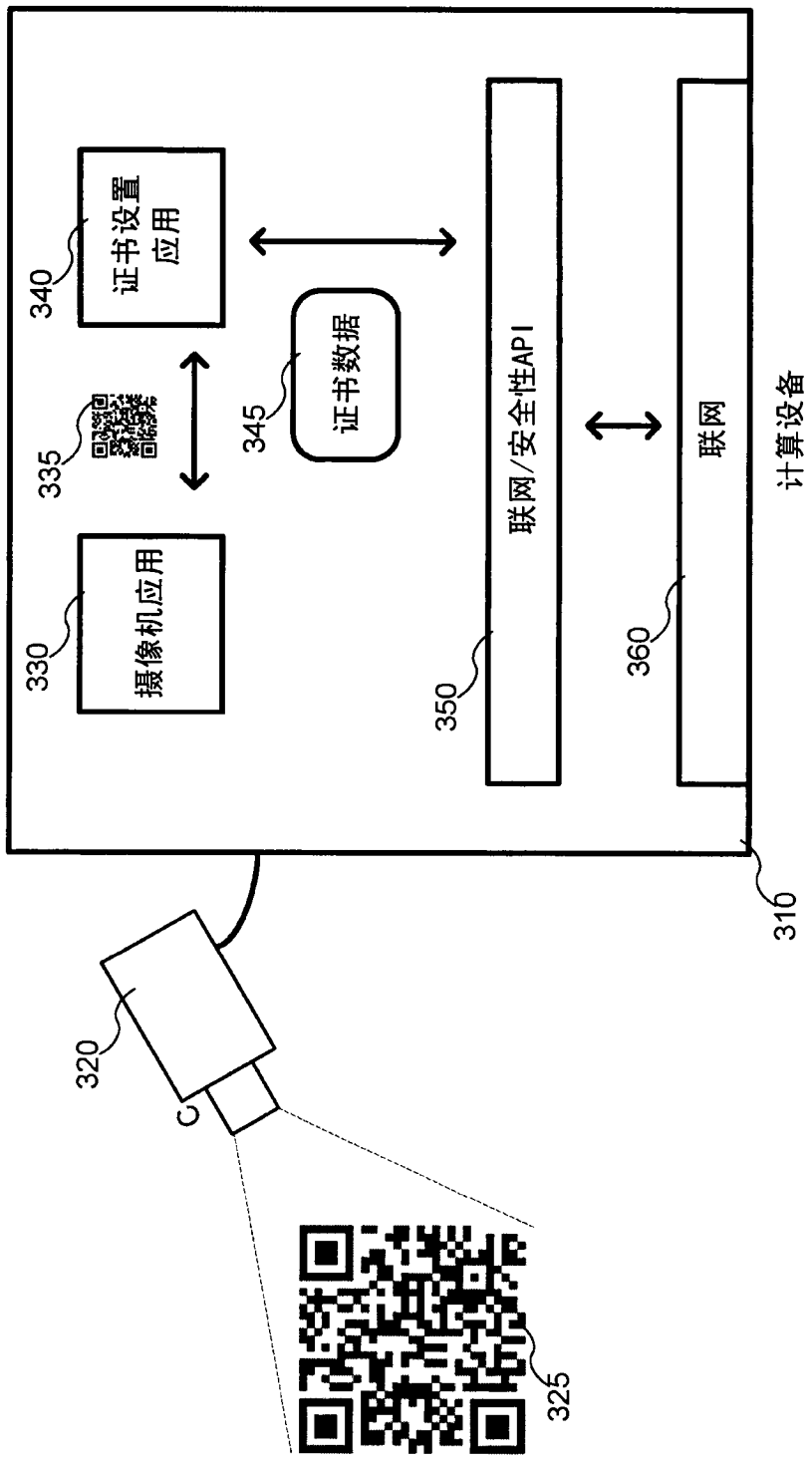

证书设置应用
340
证书数据
345
335
摄像机应用
330
联网/安全性API
350
联网
360
计算设备
310
320
C
325

图 3

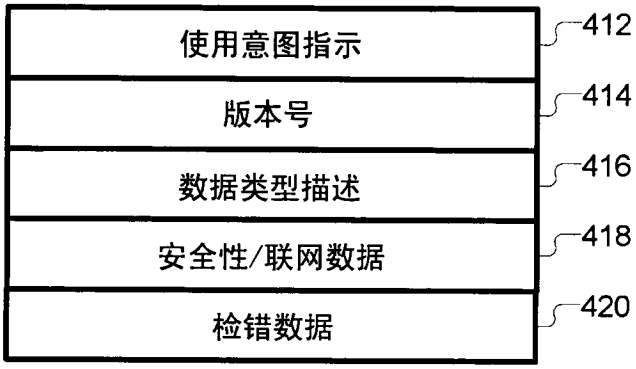

使用意图指示
412
版本号
414
数据类型描述
416
安全性/联网数据
418
检错数据
420

图 4


使用：无线设置
532
无线设置版本x. x
534
数据类型
536
网络的SSID
538
加密/协议类型
540
密钥/密码短语
542
其他网络参数
544
校验和
546

图 5a

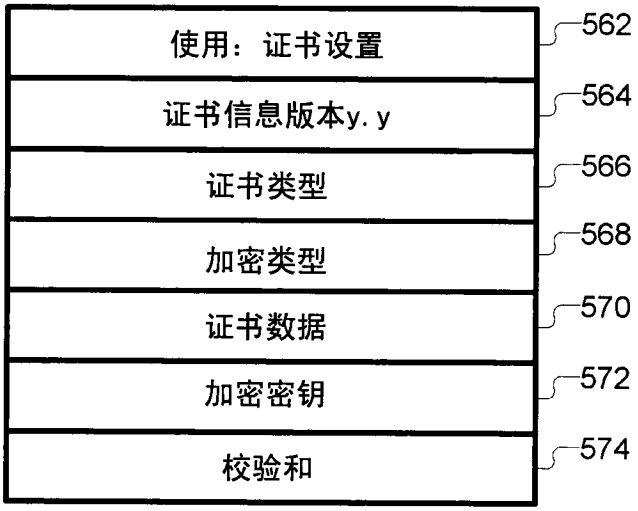

使用：证书设置
562
证书信息版本y.y
564
证书类型
566
加密类型
568
证书数据
570
加密密钥
572
校验和
574

图 5b

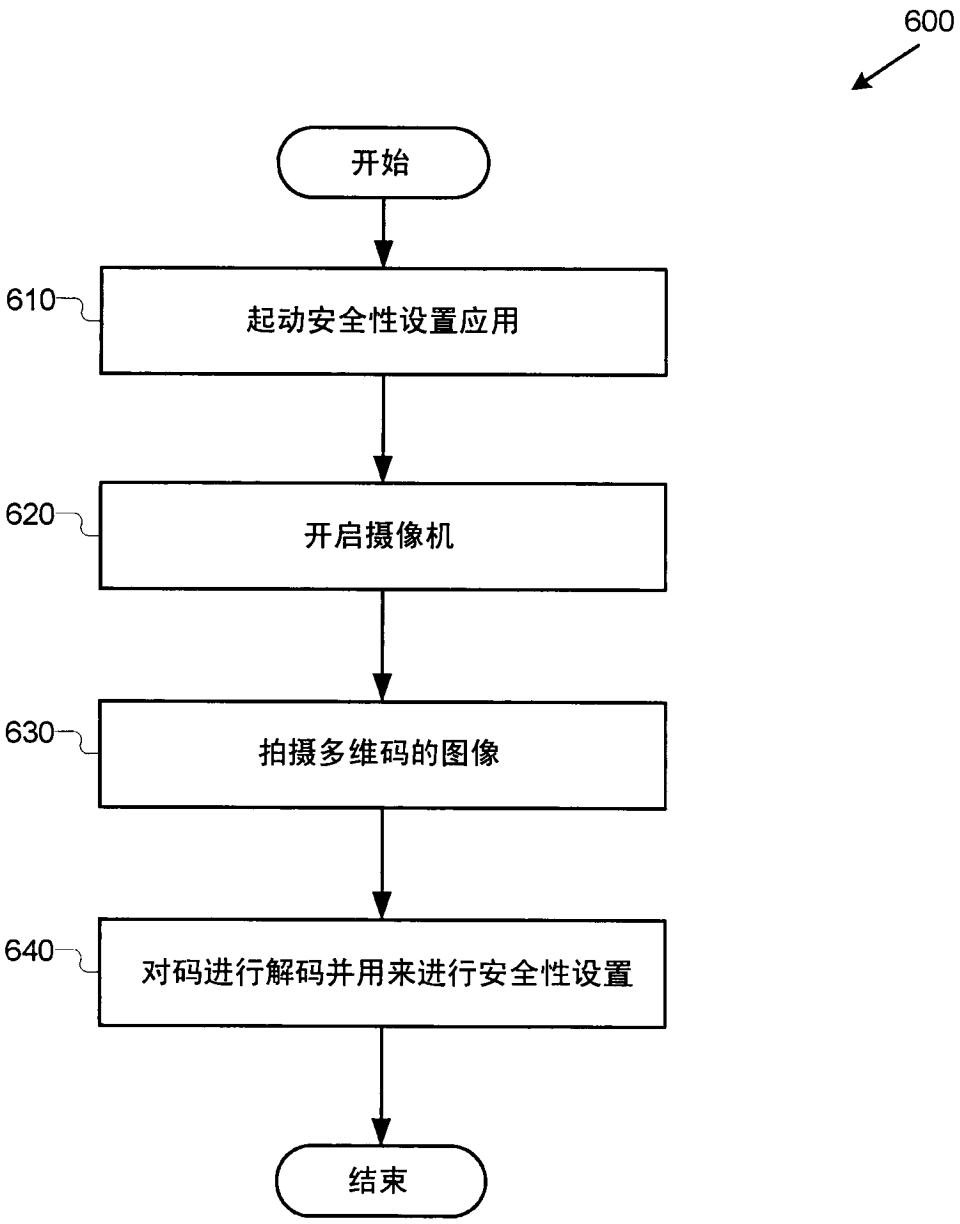

600
开始
610
起动安全性设置应用
620
开启摄像机
630
拍摄多维码的图像
640
对码进行解码并用来进行安全性设置
结束

图 6

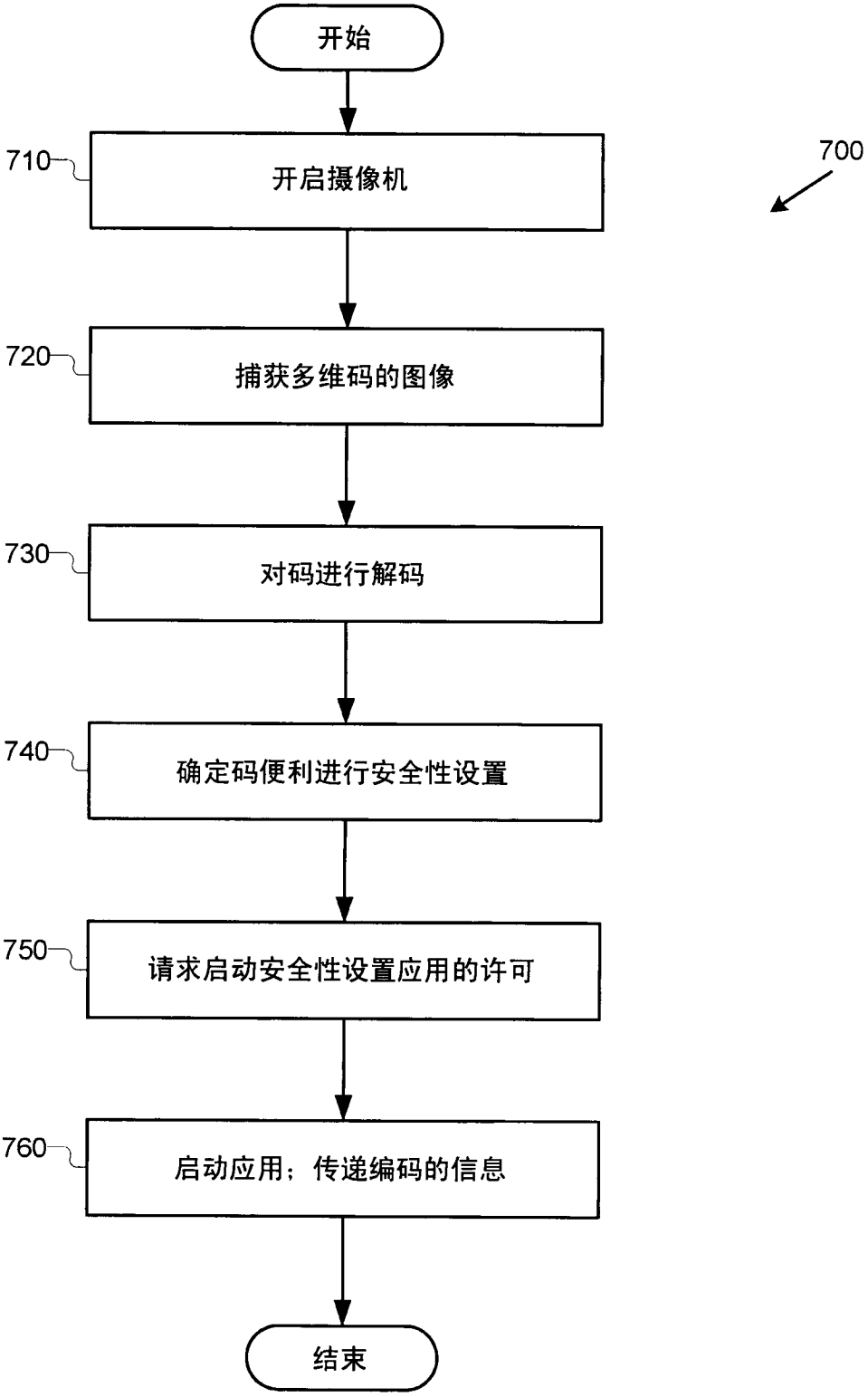

开始
710
开启摄像机
700
720
捕获多维码的图像
730
对码进行解码
740
确定码便利进行安全性设置
750
请求启动安全性设置应用的许可
760
启动应用；传递编码的信息
结束

图 7

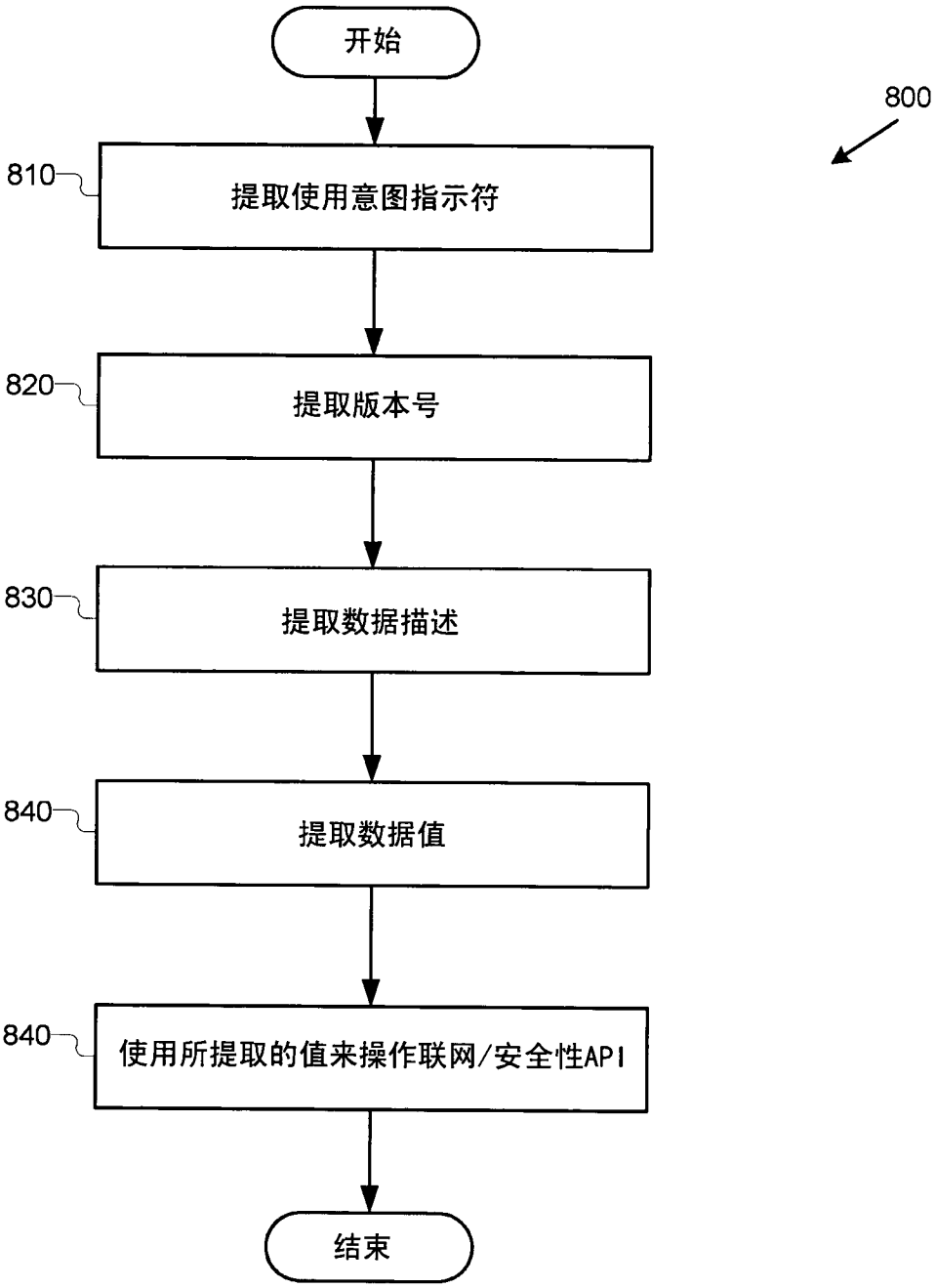

开始
800
810
提取使用意图指示符
820
提取版本号
830
提取数据描述
840
提取数据值
840
使用所提取的值来操作联网/安全性API
结束

图 8

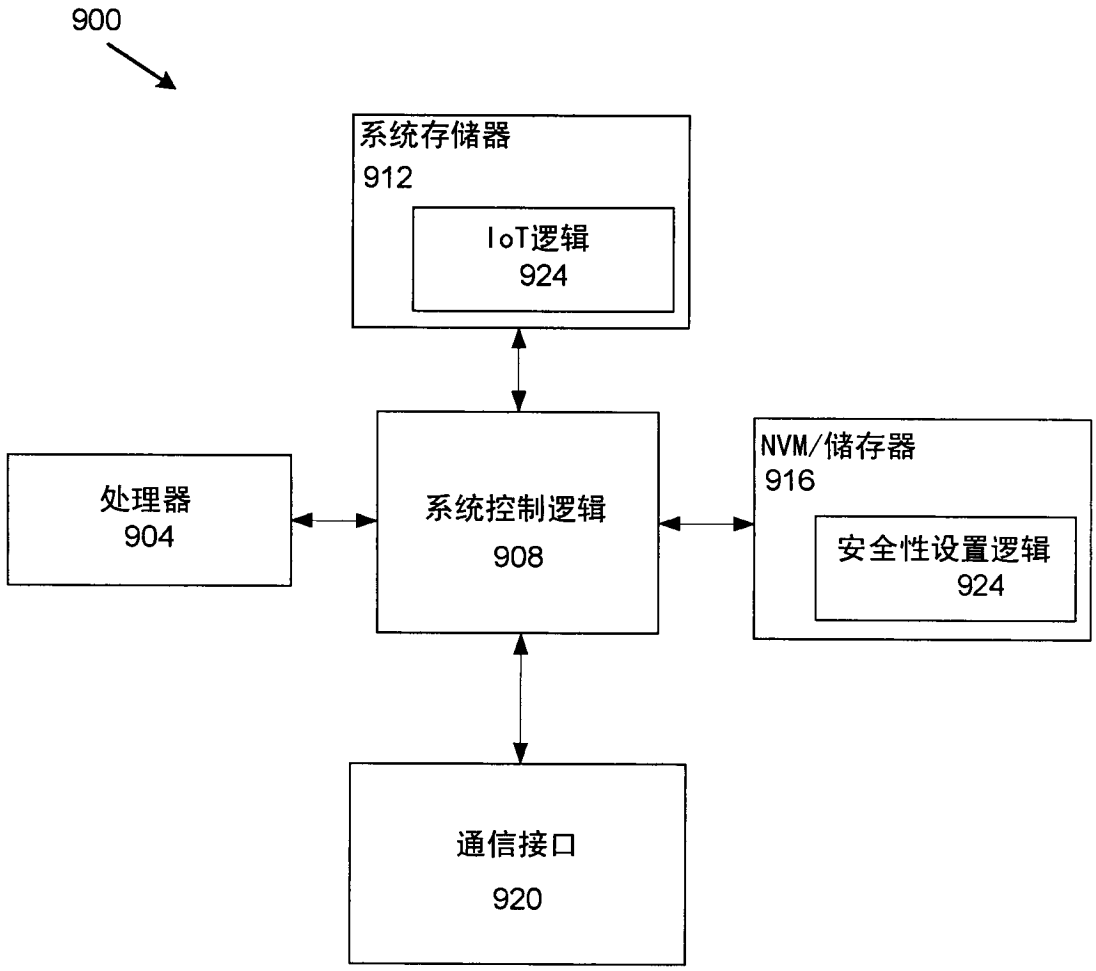

900
系统存储器
912
IoT逻辑
924
处理器
904
系统控制逻辑
908
NVM/储存器
916
安全性设置逻辑
924
通信接口
920

图 9