[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/14 (2006.01)
H04L 9/06 (2006.01)
G06F 1/00 (2006.01)

[12] 发明专利说明书

专利号 ZL 200410092041.4

[45] 授权公告日 2009 年 9 月 16 日

[11] 授权公告号 CN 100542085C

[22] 申请日 2004.11.9
[21] 申请号 200410092041.4
[30] 优先权
[32] 2003.11.10 [33] US [31] 60/518,323
[32] 2004.6.30 [33] US [31] 10/879,349
[73] 专利权人 美国博通公司
地址 美国加州
[72] 发明人 马克·布尔
[56] 参考文献
EP0583140B1 1999.12.8
CN1302404A 2001.7.4
审查员 林 姓

[74] 专利代理机构 深圳市顺天达专利商标代理有限公司
代理人 蔡晓红

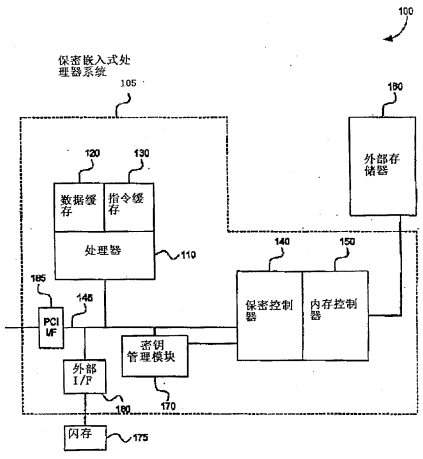
权利要求书 4 页 说明书 11 页 附图 10 页

[54] 发明名称

保密可执行编码的系统和方法

[57] 摘要

一种用于对可执行编码进行保密存储、以及将这种编码从存储器保密传送到处理器的系统和方法。 所述方法包括存储所述编码的一个加密版本。在存储装置中重加密之前，根据需要解密并解压该编码。 然后将重加密的可执行编码写入外存储器。当需要所述可执行编码的超高速缓存线时，执行一个取出动作但对其进行截取。 在截取过程中，对所述超高速缓存线进行解密。 然后将得到的纯文本超高速缓存线存储在与处理器相关联的指令超高速缓存中。



1．一种用于保密执行处理器指令的系统，其特征在于，所述系统包括：

一个第一存储器，其中包含起动代码和用第一密钥加密的可执行编码；

一个保密嵌入式处理器系统，其中包括：

一个处理器；

一个与所述处理器通讯的指令超高速缓存；

一个与所述指令超高速缓存通讯的存储器控制器；以及

一个与所述指令超高速缓存通讯的保密控制器；和

一个第二存储器，它位于所述保密嵌入式处理器系统的外部，并与所述第一存储器、存储器控制器和保密控制器通讯，

其中，所述用第一密钥加密的可执行编码被传输至所述第二存储器，被所述保密控制器解密，并由所述保密控制器使用第二密钥重加密，用所述第二密钥加密的可执行编码的一个超高速缓存线从所述第二存储器被读取，再用所述第二密钥进行解密，然后存储在所述指令超高速缓存中，以被所述处理器执行；所述保密控制器中包括：

使用高级加密标准 AES 算法重加密所述可执行编码的逻辑电路；

使用所述 AES 算法解密所述超高速缓存线的逻辑电路；

所述用于重加密所述可执行编码的逻辑电路中包括实现所述 AES 算法的密码分组链接 CBC 模式的逻辑电路；且用于解密所述超高速缓存线的逻辑电路包括实现所述 AES 算法的 CBC 模式的逻辑电路；

所述用于重加密所述可执行编码的逻辑电路中，使用所述第二存储器的一个地址作为所述 AES 算法的初始化向量，其中所述地址对应于所述超高

速缓存线在所述第二存储器中的位置；且所述用于解密所述超高速缓存线的逻辑电路中，使用所述地址作为初始化向量。

2．如权利要求 1 所述的系统，其特征在于，所述保密控制器中包括使用三重数据加密标准（3DES）算法和所述第一密钥对所述被加密的可执行编码进行解密的逻辑电路。

3．如权利要求 1 所述的系统，其特征在于，进一步包括一个密钥管理模块，其中包括：

以加密形式接收所述第一密钥的逻辑电路；

使用会话密钥对所述被加密的第一密钥进行解密的逻辑电路；

将所述第一密钥转发到所述保密控制器的逻辑电路。

4．一种提供处理器指令的保密执行的方法，其特征在于，包括以下步骤：

a. 启动处理器，以将加密编码加载到外部存储器中；

b. 使用第一加密密钥对所述加密编码中的未压缩部分进行解密，以产生解密未压缩码的第一部分；

c. 执行所述解密未压缩码的第一部分；

d. 使用所述第一加密密钥和所述解密未压缩码的第一部分对所述加密编码中的压缩部分进行解密，以产生一个可执行编码；

e. 鉴别所述可执行编码；

f. 解压缩该可执行编码从而使它占据外部存储器中的一部分，起点在第一地址并且终点在终端地址；以及

g. 执行所述可执行编码的保密执行，所述步骤 g 包括以下步骤:；

i：使用 AES 算法分别加密每一个超高速缓存线；

ii：取出一个加密超高速缓存线；

iii：截取所述取出过程；

iv：使用 AES 算法解密所取出的加密超高速缓存线；

v：确定加密超高速缓存线是否有效；

vi：如果加密超高速缓存线无效，捕获该加密超高速缓存线；和

vii：如果加密超高速缓存线有效，执行所述加密超高速缓存线；

其中，每个超高速缓存线的 AES 算法的初始化向量是超高速缓存线在外部存储器中的地址。

5．如权利要求 4 所述的方法，其特征在于，其中使用三重数据加密标准（3DES）算法执行所述解密步骤 b 和 d。

6．如权利要求 4 所述的方法，其特征在于，在执行步骤 a 以前，所述方法进一步包括以下步骤：

k．确定所述第一加密密钥是否失效，仅在所述第一加密密钥还没有失效的条件下，才执行所述步骤 a－g。

7．如权利要求 4 所述的方法，其特征在于，在执行步骤 a 以前，所述方法进一步包括以下步骤：

h．产生加密编码。

8．如权利要求 7 所述的方法，其特征在于，所述步骤 h 中包括：

i．压缩所述可执行编码；

ii．对所述可执行编码进行散列处理以产生一个散列值；

iii．加密所述可执行编码；

iv．存储所述加密的可执行编码。

9．如权利要求 8 所述的方法，其特征在于，所述步骤 ii.中，使用保密散列算法 1（SHA-1）对所述可执行编码进行散列处理。

保密可执行编码的系统和方法

技术领域

本发明涉及信息保密，特别涉及保密处理。

背景技术

计算平台内的保密处理是公知的普通问题。特别是可执行编码的任何无意或非期望的改变，都会产生可怕的运行结果。例如，恶意编码可被（例如，特洛依木马）插入到可执行编码中，从而使处理器执行非期望和/或无法预测的操作。换句话说，敌对用户可以改变指令的次序，从而由出故障的处理器来执行操作。此时，其结果可能也是非期望的。其他的威胁可能不是恶意的。例如，存储器硬件的故障可能会改变可执行编码。显然，这会影响处理器的运行和它的结果。

另外，保密是一个与可编程逻辑电路自身相关的问题。可执行编码其本身是必须作为秘密而保存的信息。对可执行编码的披露会对敏感数据产生非期望的损害。一般而言，可执行编码在存储时、以及在存储器与处理器或它的超高速缓存之间传送时，容易被损坏。

考虑到这种已知的威胁和脆弱性，需要一种可克服以上情况的系统和方法，从而使处理器只执行所需要的操作，并保持其程序的机密性。

发明内容

本发明提供描述了可执行编码的保密存储和这种编码从存储器到处理器的保密传送。本发明包括编码的加密版本的存储。在存储装置（如闪存）中重

加密之前，可根据需要解密并解压该编码。然后将重加密的可执行编码写入外存储器。当需要可执行编码的超高速缓存线时，执行一个取出动作但对其进行截取。在截取过程中，对所述超高速缓存线进行加密。然后将得到的纯文本超高速缓存线存储在一个与处理器相关联的指令超高速缓存中。

一方面，本发明提供了一种用于保密执行处理器指令的系统，所述系统包括：

一个第一存储器，其中包含起动代码和用第一密钥加密的图像；

一个保密嵌入式处理器系统，其中包括：

一个处理器；

一个与所述处理器通讯的指令超高速缓存；

一个与所述指令超高速缓存通讯的存储器控制器；以及

一个与所述指令超高速缓存通讯的保密控制器；和

一个第二存储器，它位于所述保密嵌入式处理器系统的外部，并与所述第一存储器、存储器控制器和保密控制器通讯，

其中，所述用第一密钥加密的图像被传输至所述第二存储器，被所述保密控制器解密，并由所述保密控制器使用第二密钥再加密，用所述第二密钥加密的图像的一个超高速缓存线从所述第二存储器被读取，再用所述第二密钥进行解密，然后存储在所述指令超高速缓存中，以被所述处理器执行。

优选地，所述保密控制器中包括使用三重数据加密标准（3DES）算法和所述第一密钥对所述被加密图像进行解密的逻辑电路。

优选地，所述系统中进一步包括一个密钥管理模块，其中包括：

以加密形式接收所述第一密钥的逻辑电路；

使用会话密钥对所述被加密的第一密钥进行解密的逻辑电路；

将所述第一密钥转发到所述保密控制器的逻辑电路。

优选地，所述保密控制器中包括：

使用高级加密标准（AES）算法重加密所述图像的逻辑电路；以及

使用所述 AES 算法解密所述超高速缓存线的逻辑电路。

优选地，所述用于重加密所述图像的逻辑电路中，包括实现所述 AES 算法的密码分组链接（CBC）模式的逻辑电路；且

所述用于解密所述超高速缓存线的逻辑电路中，包括实现所述 AES 算法的 CBC 模式的逻辑电路。

优选地，所述用于重加密所述图像的逻辑电路中，包括实现所述 AES 算法的所述 CBC 模式的解密模式的逻辑电路；且

所述用于解密所述超高速缓存线的逻辑电路中，包括实现所述 AES 算法的所述 CBC 模式的加密模式的逻辑电路。

优选地，所述用于重加密所述图像的逻辑电路中，使用所述第二存储器的一个地址作为所述 AES 算法的初始化向量（IV），其中所述地址对应于所述超高速缓存线在所述第二存储器中的位置；且

所述用于解密所述超高速缓存线的逻辑电路中，使用所述地址作为所述初始化向量。

另一方面，本发明提供一种提供处理器指令的保密执行的方法，包括：

a. 启动处理器，以将加密编码加载到外部存储器中；

b. 使用图像密钥对所述加密编码中的未压缩部分进行解密，以产生解密未压缩码的第一部分；

c. 执行所述解密未压缩码的第一部分；

d. 使用所述图像密钥对所述加密编码中的压缩部分进行解密，以产生一

个图像；

e. 鉴别所述图像；

f. 解压缩该图像从而使它占据外部存储器中的一部分，起点在第一地址并且终点在终端地址；以及

g. 执行所述图像的保密执行。

优选地，其中其中使用三重数据加密标准（3DES）算法执行所述解密步骤 b 和 d。

优选地，在执行步骤 a 以前，所述方法进一步包括以下步骤：

h. 确定所述图像密钥是否失效，仅在所述图像密钥还没有失效的条件下，才执行所述步骤 a—g。

优选地，在执行步骤 a 以前，所述方法进一步包括以下步骤：

h. 产生加密编码。

优选地，所述步骤 h 中包括：

i. 压缩所述图像；

ii. 对所述图像进行散列处理以产生一个散列值；

iii. 加密所述图像；

iv. 存储所述加密编码。

优选地，所述步骤 h.ii.中，使用保密散列算法 1（SHA-1）对所述图像进行散列处理。

优选地，所述步骤 h.iii.中，使用三重数据加密标准（3DES）算法加密图像。

优选地，所述步骤 h.iv.中，将加密编码存储到闪存中。

优选地，步骤 a 包括：

i. 将处理器的状态复位；

ii. 加载图像密钥；

iii. 将加密编码传输入外部存储器；和

iv. 将处理器切换到保密模式。

优选地，所述外部存储器包括双数据速率同步动态随机访问存储器（DDR-SDRAM）。

优选地，所述步骤 a.iv.中包括：

A. 清除处理器的状态；

B. 将与处理器相关联的一个指令超高速缓存设置为无效状态；以及

C. 将图像的执行限制在外部存储器的一部分。

优选地，所述步骤 g 包括：

i. 分别加密图像的每一个超高速缓存线；

ii. 取出一个加密超高速缓存线；

iii. 截取所述取出过程；

iv. 解密所取出的加密超高速缓存线；

v. 确定加密超高速缓存线是否有效；

vi. 如果加密超高速缓存线无效，捕获该加密超高速缓存线；和

vii. 如果加密超高速缓存线有效，执行所述加密超高速缓存线。

优选地，所述图周 g.i.中，使用高级加密标准（AES）加密每一个超高速缓存线，所述步骤 g.iv.中，使用 AES 算法解密取出的加密超高速缓存线。

优选地，所述 AES 算法使用于密码分组链接（CBC）模式。

优选地，所述步骤 g.i.中，使用 AES 算法加密每个超高速缓存线，所述步骤 g.iv.中，使用 AES 算法的加密模式解密取出的加密超高速缓存线。

优选地，每个超高速缓存线的 AES 算法的初始化向量（IV）是超高速缓存线在外部存储器中的地址。

附图说明

图 1 是一个原理框图，其中示出了本发明一个实施例的总体结构。

图 2 是本发明一个实施例中可执行编码在闪存内处于加密和压缩形式时的示意图。

图 3 是本发明一个实施例中包含有解密和解压缩的可执行编码的外部存储器的示意图。

图 4 示出了本发明一个实施例中的取出过程，其中将编码的超高速缓存线解密并转发到指令超高速缓存。

图 5 是本发明一个实施例中加密图像的产生流程图。

图 6 是本发明一个实施例中访问并使用加密图像的总体流程图。

图 7 是本发明一个实施例中处理器启动过程的详细流程图。

图 8 是本发明一个实施例中切换到保密模式的流程图。

图 9 是本发明一个实施例中保密执行过程的流程图。

图 10 是本发明方法的一个简化版本的流程图。

具体实施方式

现在参照附图描述本发明的较佳实施例，其中的标号表示相同或功能相似的元件。在附图中，每个标号最左侧的位对应于第一次使用标号的附图。对于其中描述的具体配置和设备，应该理解仅是出于示意的目的。相关领域的技术人员可在不脱离发明宗旨和范围的条件下，使用其它的配置和设备。对于相关领域的技术人员而言，本发明显然也可以用于多种装置、系统和应用程序。

Ⅰ. 概述

现在参照附图描述本发明的较佳实施例，其中的标号表示相同或功能相似的元件。在附图中，每个标号最左侧的位数对应于第一次使用标号的图。对于其中描述的具体配置和设备，应该理解仅是出于示意的目的。相关领域的技术人员可在不脱离发明宗旨和范围的条件下，使用其它的配置和设备。对于相关领域的技术人员而言，本发明显然也可以用于多种装置、系统和应用程序。

II．系统

本发明提供了一种与存储器模块通讯的保密嵌入式处理器系统。图 1 示出了本发明的一个实施例。图中，保密嵌入式处理器系统 105 与外部存储器模块 160 及闪存模块 175 相连。闪存模块 175 以压缩和加密的形式存储可执行编码（在下文中称为图像）。由如下的详细描述可知，在启动过程中，加密压缩的图像被传输至外部存储器 160。然后，该图像被解密、解压缩，然后被重加密并存储在外部存储器 160 中。

对于将被处理器 110 执行的指令，每一次从外部存储器 160 中取出它的一个超高速缓存线。然而，该取出过程会被存储器控制器 150 所截取。在将取出的超高速缓存线加载到指令超高速缓存 130 之前，由保密控制器 140 将其解密。

如图所示，在保密嵌入式处理器系统 105 中有一个密钥管理模块 170，它为保密控制器 140 提供密钥管理服务。在本发明的一个实施例中，还可提供一个外部接口 180，以实现闪存 175 与系统 105 之间的相连。还可提供一个外设部件互连（PCI）接口 185，以实现与保密嵌入式处理器系统 105 的通讯。PCI 接口 185、外部接口 180、密钥管理模块 170、保密控制器 140、以及处理器 110 通过诸如总线的基础结构 145 相互连接。

图 2 中更详细地示出了闪存 175。在图 2 中，示出了当图像驻留于闪存 175

内时图像的结构。该图像包括一段启动码 210。接下来是两个码块 220 和 230。用第一加密密钥，这里称为图像密钥，对这两个码块集体地加密。在本发明一个实施例中，使用三重数据加密标准（3DES）算法对这些码块进行加密。在图示实施例中，码块 220 包括用于解密剩余码块 230 所需的逻辑。应该注意，在图示实施例中，码块 230 是压缩的。码块 240 代表由码块 210、220 和 230 得到的鉴别码。码块并不是图像本身的一部分。在图示实施例中，所述鉴别过程是一个散列消息鉴别码（HMAC）过程。

图 3 示出了当图像被解密并解压缩后，驻留于外部存储器 160 时的图像结构。如图所示，块 330 中占据了存储器的 10KB 存储容量。该存储间隔的初始地址为 310。该间隔的终端地址为 320。在本发明的一个实施例中，该起始地址 310 和终端地址 320 被转发到存储器控制器 150。以起到保密检验作用，从而不允许执行这些边界以外的指令。

图 4 示出了从外部存储器 160 取出指令时的流程和过程。当图像被解密后，使用第二密钥将图像重加密以形成重加密图像 410。然后基于超高速缓存线取出所述重加密图像 410。出于解密目的，由解密逻辑电路 440 找到并读取超高速缓存线 420。在图示实施例中，超高速缓存线 420 的地址 430 用于初始化解密过程。在本发明的一个实施例中，重加密过程按密码分组链接（CBC）模式，使用高级加密标准（AES）算法。此外，在本发明的一个实施例中，重加密过程在解密模式中可使用 AES/CBC 过程。结果，在该实施例中，解密过程 440 实际上使用 AES 的加密模式。然后将得到的纯文本超高速缓存线 450 转发到指令超高速缓存 130。最终由处理器 110 执行该纯文本超高速缓存线。

如图 1 所示，密钥管理模块 170 处理一部分与加密密钥的保护相关的管理和保密功能。特别地，在本发明的一个实施例中，保密嵌入式处理器系统 105

以加密形式接收图像密钥。密钥管理模块 170 使用会话密钥将加密图像密钥解密。从而使保密控制器 140 如上所述那样使用所得到的纯文本图像密钥。

此外，可将一个时间限制与所述图像密钥相关联，从而只能在给定的持续时间内或者某个特定的时间点使用该图像密钥。在这个时间点过后，该密钥不能够再使用，被称为失效。在本发明的一个实施例中，保密控制器 140 在使用该密钥前会校验图像密钥是否已经失效。当然，也可以在密钥管理模块 170 中执行该校验。

III. 方法

图 5 示出了当图像被存储在闪存中时的初始压缩和加密过程。该过程开始于步骤 510。在步骤 520 中，将图像压缩。在步骤 530 中，对图像进行散列处理以产生一个 HMAC。在本发明的一个实施例中，使用了保密散列算法 1（SHA-1）。在步骤 540 中，使用图像密钥将压缩图像加密。如上文提到的，可使用 3DES 算法执行该加密。在步骤 550 中，将得到的压缩加密图像存储在闪存中。本过程在步骤 560 结束。

图 6 示出了保密地访问和执行图像的总体过程。本过程开始于步骤 610。在步骤 620 中，处理器经历其启动操作。在步骤 630 中，使用图像密钥对图像的已解压缩部分进行解密。在步骤 640 中，执行该解压缩码。所述编码之解压缩码部分中的逻辑用于对剩余图像进行解密。在步骤 650 中，使用图像密钥对图像的剩余部分进行解密。在步骤 660 中，鉴别所述图像。如上所述，可使用 SHA-1 算法执行鉴别。在步骤 670 中，将图像解压缩。在步骤 680 中，开始保密执行。本过程在步骤 690 结束。

图 7 更详细地示出了处理器的启动步骤（即图 6 的步骤 620）。本过程开

始于步骤 710。在步骤 720 中，将装置状态复位。在步骤 730 中，出于顺序加密处理的目的，加载加密编码。在步骤 740 中，将图像从闪存移动到外部存储器。在本发明的一个实施例中，可使用双数据速率同步动态随机访问存储器（DDR-SDRAM）实现外部存储器。在步骤 750 中，将系统切换到保密模式。本过程在步骤 760 结束。

图 8 更详细地示出了切换到保密模式的步骤（即图 7 的步骤 750）。本过程开始于步骤 810。在步骤 820 中，清除处理器状态。在步骤 830 中，将与处理器相关联的指令和数据超高速缓存设为无效状态。这可防止任何恰好驻留于这些缓存内的信息被处理器所执行。在步骤 840 中，将图像的上方和下方的地址界转发到存储器控制器，从而将执行限制在 DDR-SRAM 的下方 n 千字节。本过程在步骤 850 结束。

图 9 更详细地示出了保密执行的步骤（图 6 的步骤 680）。本过程开始于步骤 910。在步骤 915 中，使用基于每一个超高速缓存线的会话密钥对图像进行加密。在本发明的一个实施例中，本步骤使在 CBC 模式下用 AES 算法。此外，还可以此加密过程中使用 AES 的解密配置。这提供了整个图像加密过程中的错误校验。在步骤 920 中，将加密图像写入外部存储器。在步骤 925 中，取出一个指令超高速超高速缓存线，所述指令超高速缓存线是在地址边界内被取出的。在步骤 930 中，所述取出被存储器控制器所截取。在步骤 935 中，由保密控制器对该超高速缓存线进行解密。如果加密过程按解密模式使用 AES/ CBC 算法，那么解密步骤 935 实际上会使用 AES/ CBC 的加密模式。在步骤 935 对超高速缓存线进行解密之后，会在步骤 940 中确定得到的指令是否有效。如果无效，则在步骤 945 捕获该指令。否则，该指令准备在步骤 955 中执行。在步骤 960 中，将确定是否有需要取出并执行的附加指令，或者确定本过程是

否中止。如果本过程已中止，则过程在步骤 950 结束。否则过程返回步骤 925，以取出附加的超高速缓存线。

图 10 示出了本发明的另一种方法。本过程开始于步骤 1005。在步骤 1010 中，从单板只读存储器（ROM）发起启动过程。在步骤 1015 中，将启动编码提交给保密模块。在步骤 1020 中，散列该启动码。在本步骤中，保密模块会保持该散列值。在步骤 1025 中，开始执行启动码。在步骤 1030 中，对压缩码进行压缩，从而使保密模块保持其得到的缓存值。在步骤 1035 中，标记散列值。在步骤 1040 中，将加密图像传输到外部存储器。如上所述，在本发明的一个实施例中，外部存储器可用 DDR-SRAM 实现。在步骤 1045 中，使用图像密钥解密所述解压缩码。在步骤 1050 中，执行该解压缩码。在步骤 1055 中，用图像密钥将剩余图像解密。在步骤 1060 中，根据需要对剩余图像进行解密。本过程在步骤 1065 结束。

Ⅳ. 结论

虽然以上描述了本发明的不同实施例，应该理解它们是以示例而不是以限制的方式提出的。对于本领域的技术人员而言，显然能够在不脱离本发明宗旨和范围的条件下，做出各种改变和细化。因此，本发明不应局限于以上所描述的任何示例性实施例。

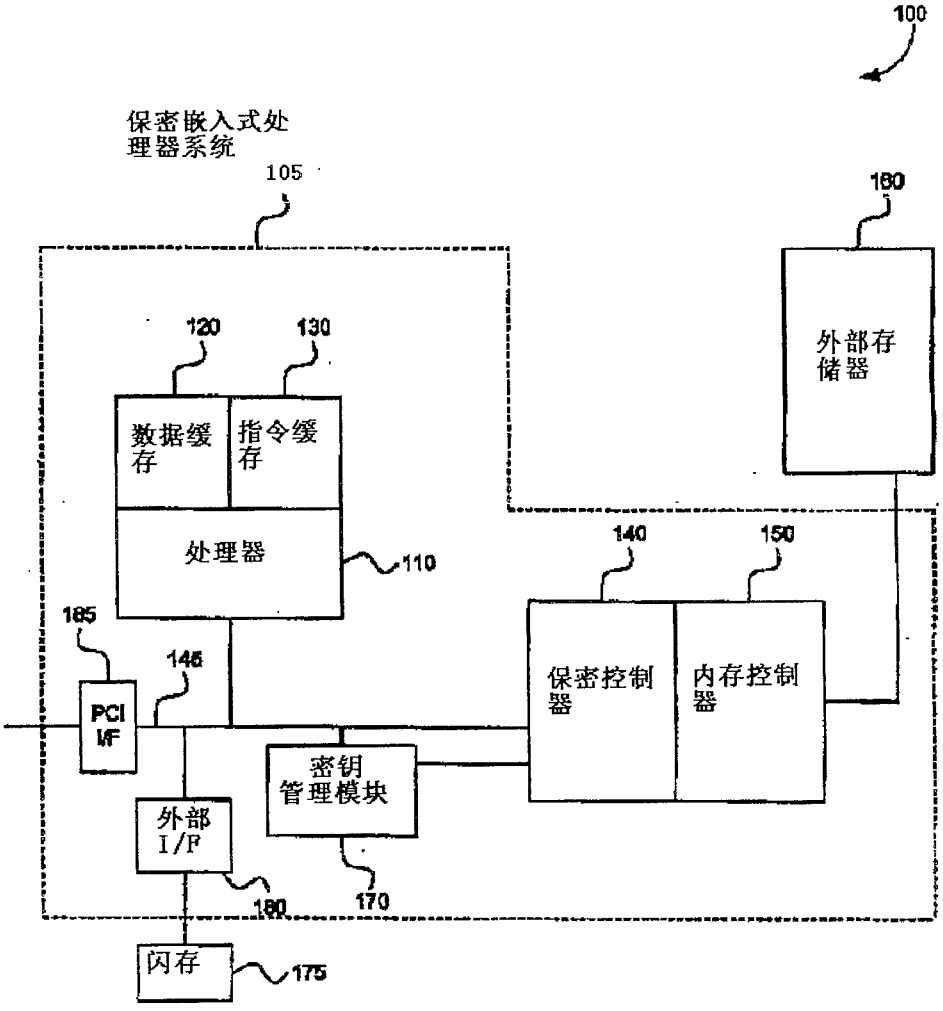

100
保密嵌入式处理器系统
105
160
外部存储器
120
130
数据缓存
指令缓存
处理器
110
140
150
保密控制器
内存控制器
185
145
PCI I/F
密钥管理模块
外部I/F
180
170
闪存
175

图1

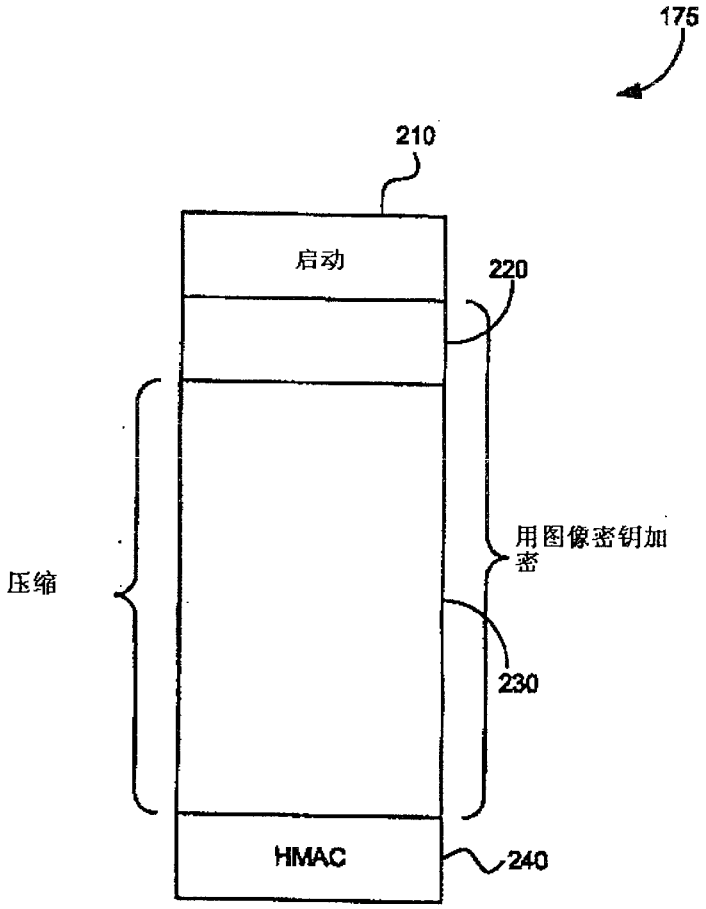


图2

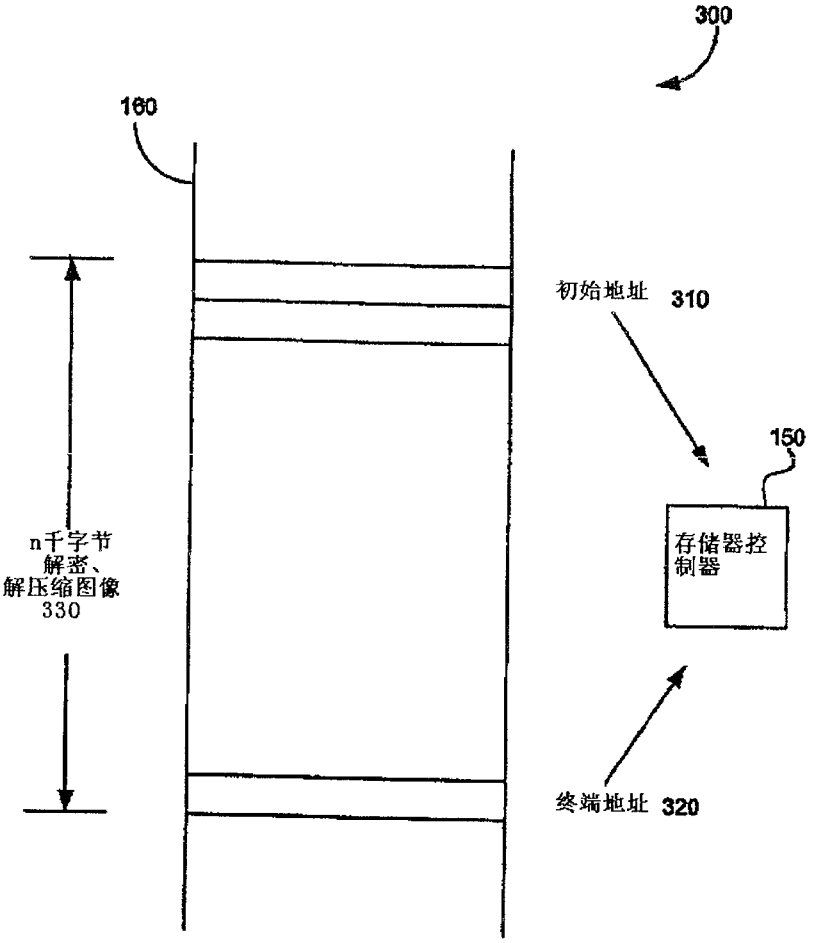


图3

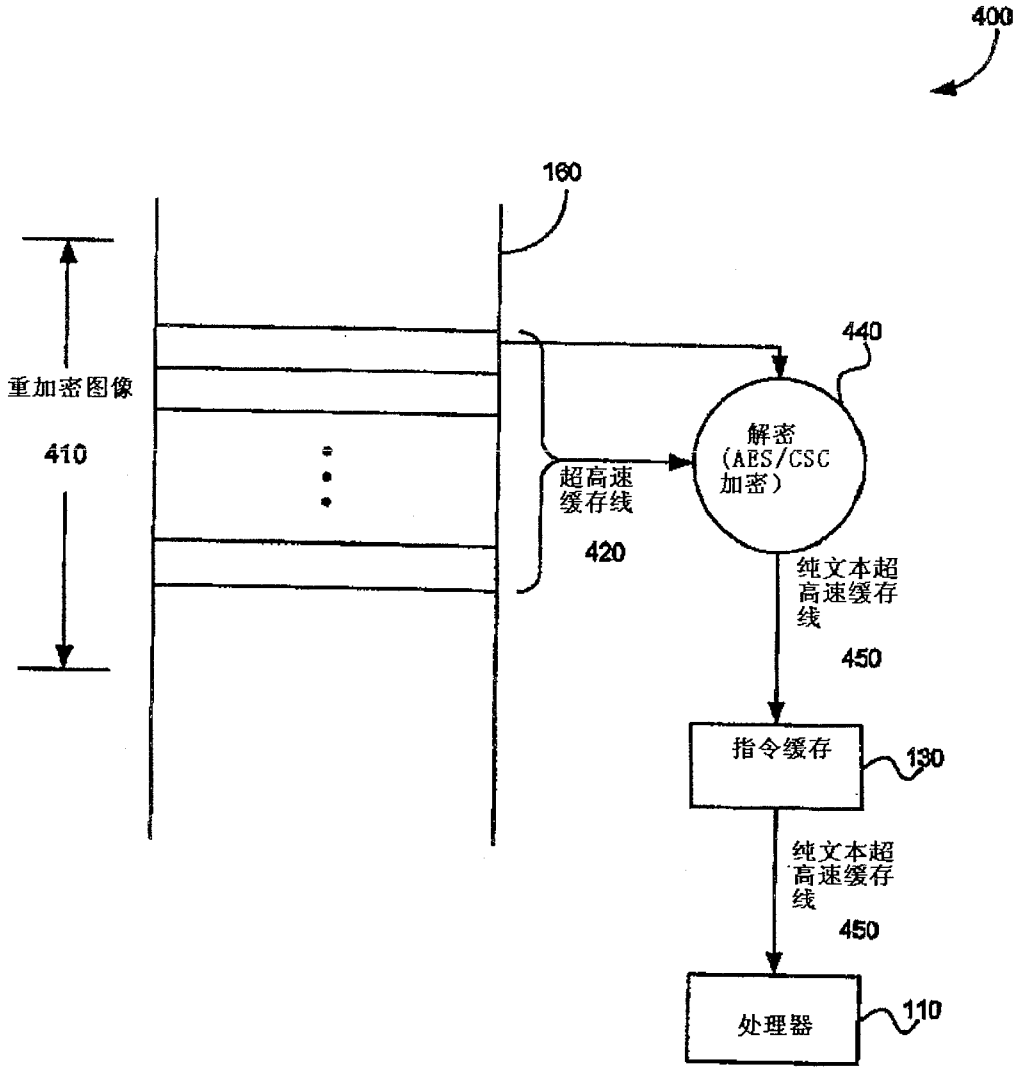

400
160
重加密图像
410
超高速
缓存线
420
440
解密
(AES/CSC
加密)
纯文本超
高速缓存
线
450
指令缓存
130
纯文本超
高速缓存
线
450
处理器
110

图4

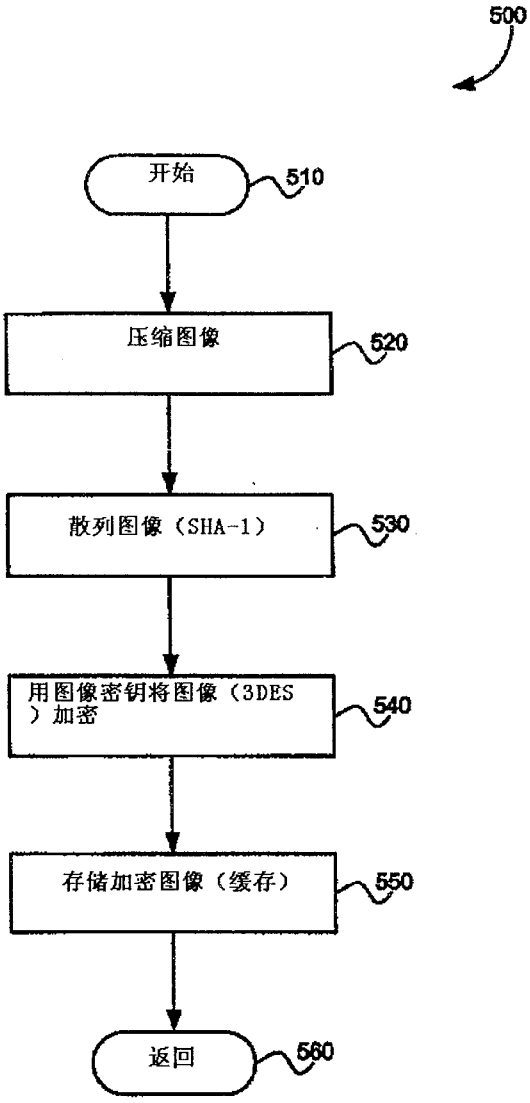

500
开始
510
压缩图像
520
散列图像（SHA-1）
530
用图像密钥将图像（3DES）加密
540
存储加密图像（缓存）
550
返回
560

图5

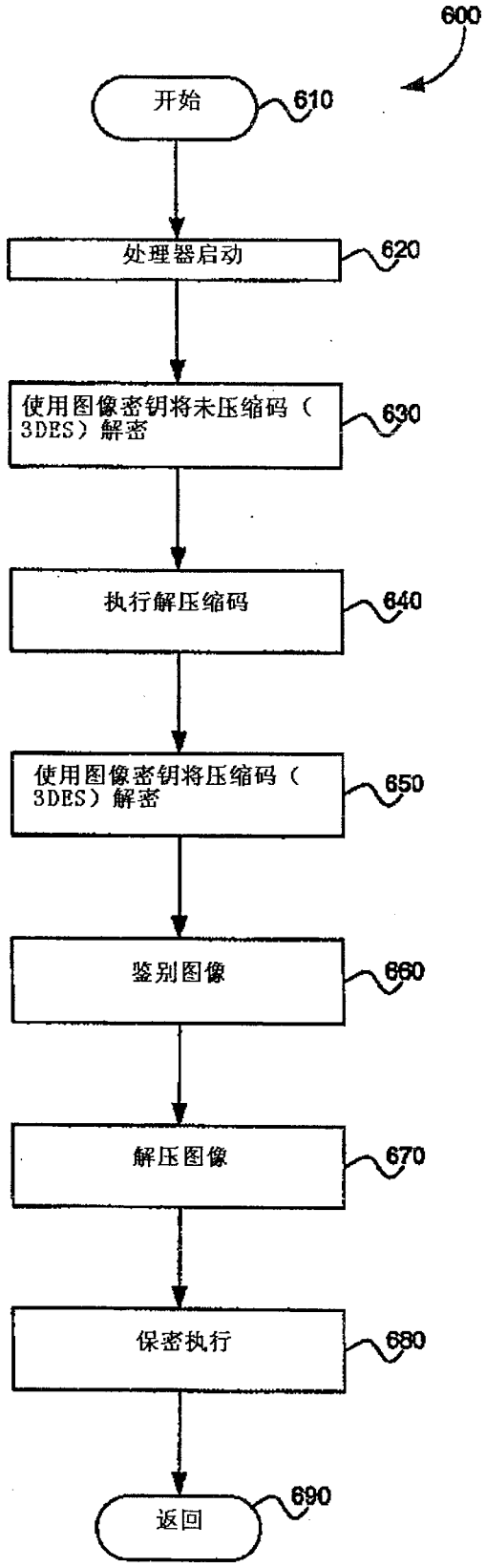

600
开始
610
处理器启动
620
使用图像密钥将未压缩码（3DES）解密
630
执行解压缩码
640
使用图像密钥将压缩码（3DES）解密
650
鉴别图像
660
解压图像
670
保密执行
680
返回
690

图6

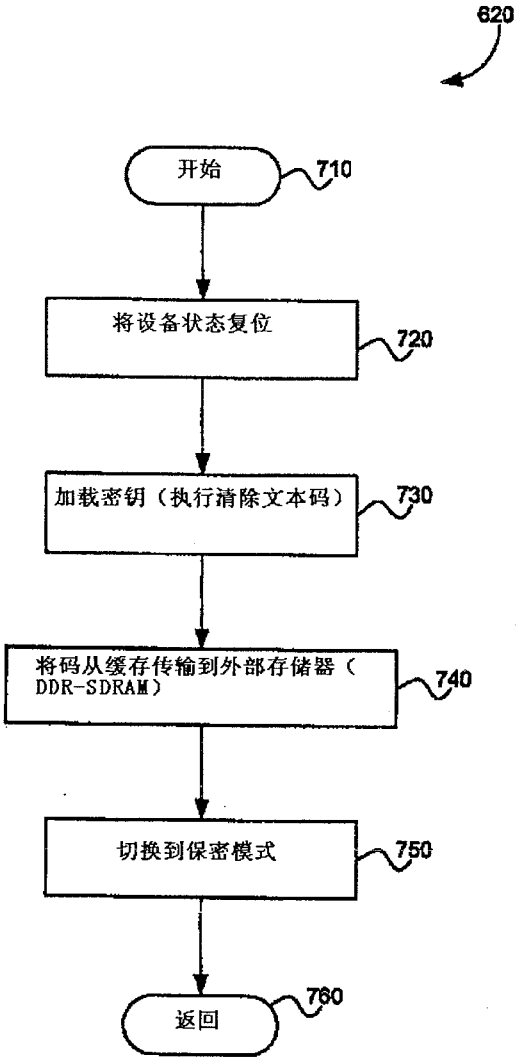

620
开始
710
将设备状态复位
720
加载密钥（执行清除文本码）
730
将码从缓存传输到外部存储器（DDR-SDRAM）
740
切换到保密模式
750
返回
760

图7

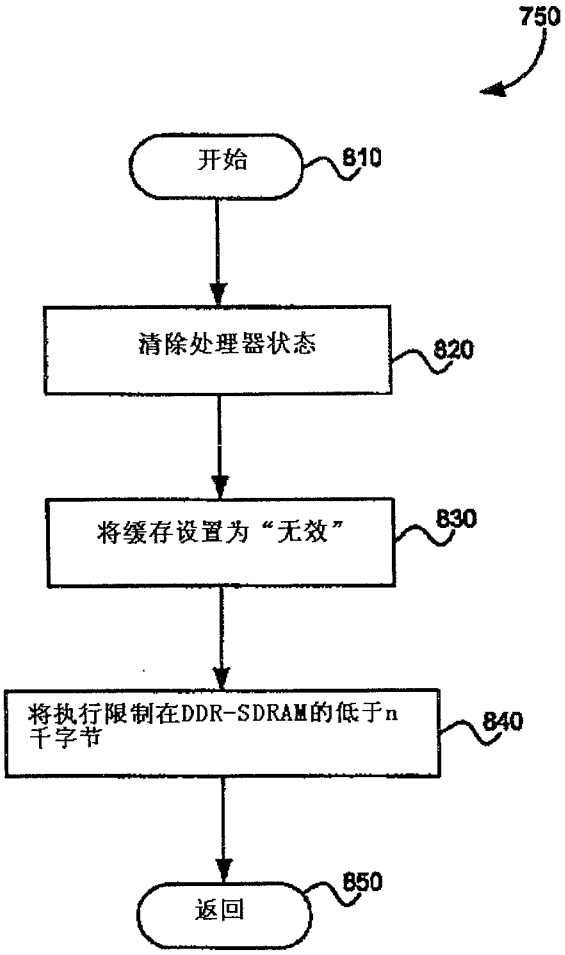

750
开始
810
清除处理器状态
820
将缓存设置为“无效”
830
将执行限制在DDR-SDRAM的低于n千字节
840
返回
850

图8

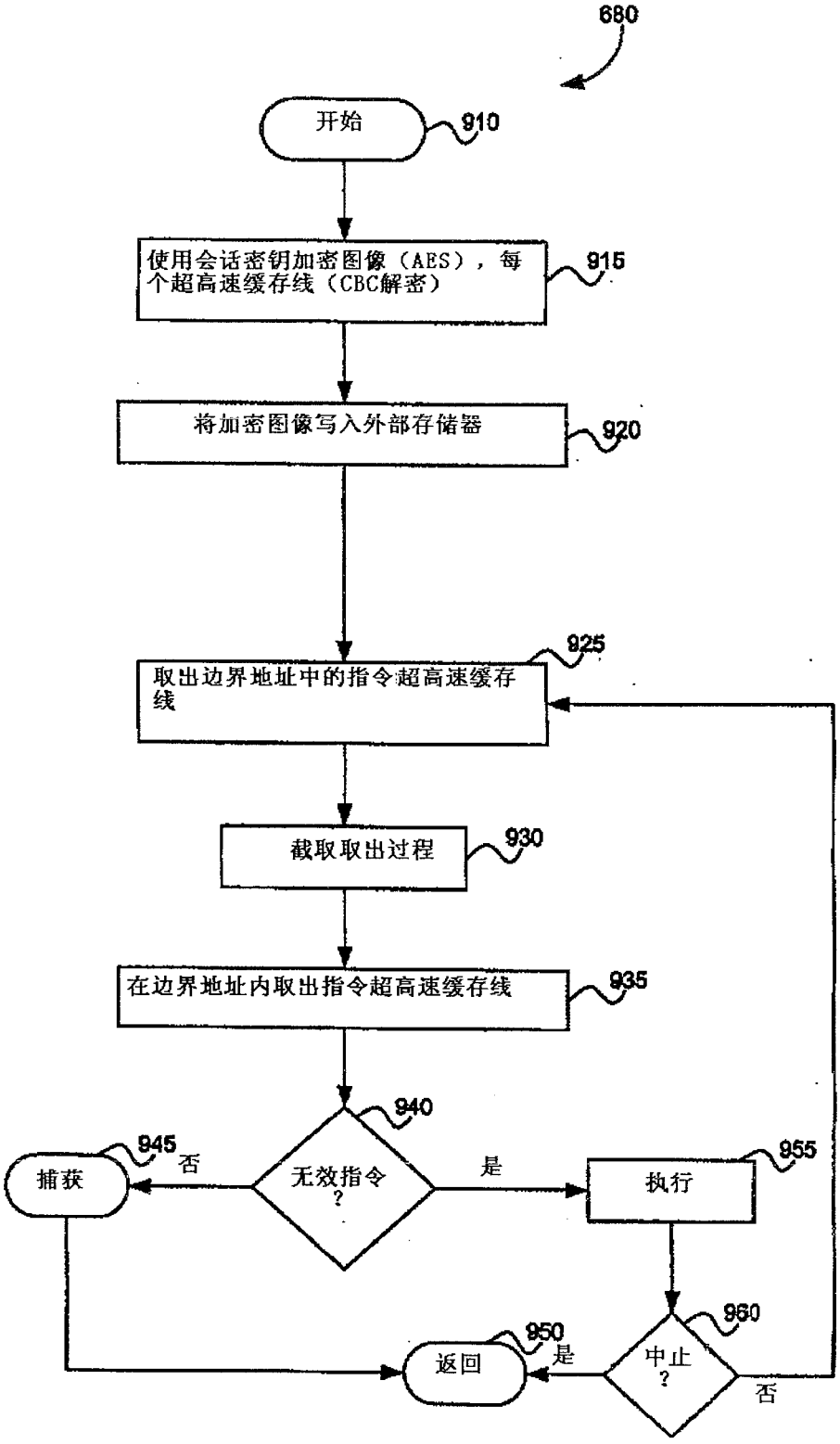

680
开始
910
使用会话密钥加密图像（AES），每个超高速缓存线（CBC解密）
915
将加密图像写入外部存储器
920
取出边界地址中的指令超高速缓存线
925
截取取出过程
930
在边界地址内取出指令超高速缓存线
935
940
无效指令？
否
是
捕获
945
执行
955
中止？
960
是
否
返回
950

图9

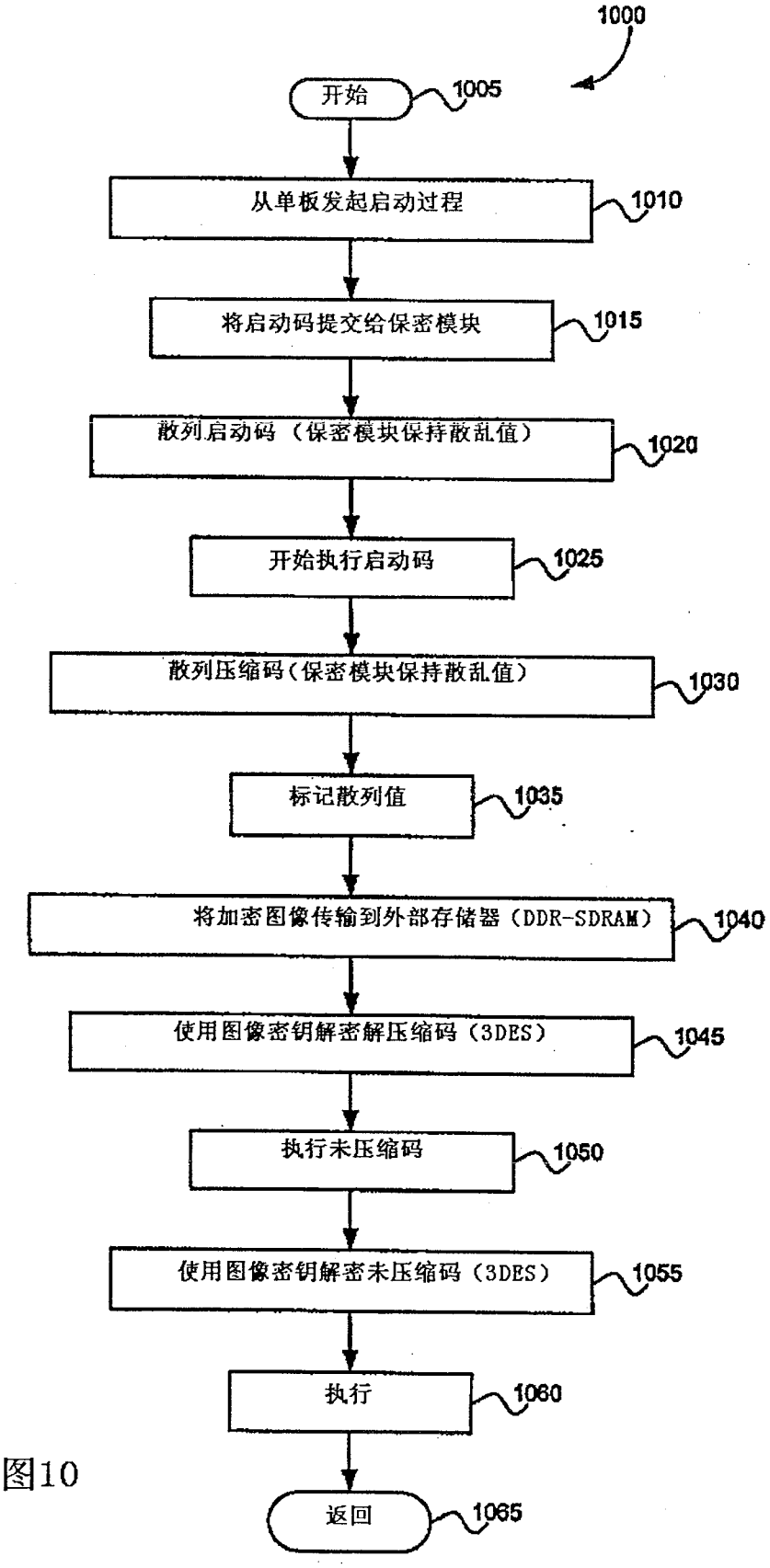

1000
开始
1005
从单板发起启动过程
1010
将启动码提交给保密模块
1015
散列启动码（保密模块保持散乱值）
1020
开始执行启动码
1025
散列压缩码（保密模块保持散乱值）
1030
标记散列值
1035
将加密图像传输到外部存储器（DDR-SDRAM）
1040
使用图像密钥解密解压缩码（3DES）
1045
执行未压缩码
1050
使用图像密钥解密未压缩码（3DES）
1055
执行
1060
返回
1065

图10