



(12)发明专利

(10)授权公告号 CN 104272752 B

(45)授权公告日 2017.12.15

(21)申请号 201380023859.8

史蒂文·约翰·哈尔特

(22)申请日 2013.04.16

(74)专利代理机构 北京律盟知识产权代理有限公司
11287

(65)同一申请的已公布的文献号
申请公布号 CN 104272752 A

代理人 宋献涛

(43)申请公布日 2015.01.07

(51)Int.Cl.

(30)优先权数据

H04N 21/426(2011.01)

61/645,577 2012.05.10 US

H04N 21/438(2011.01)

13/715,351 2012.12.14 US

H04N 21/44(2011.01)

H04N 21/4405(2011.01)

(85)PCT国际申请进入国家阶段日
2014.11.06

H04N 21/443(2011.01)

H04N 21/835(2011.01)

(86)PCT国际申请的申请数据
PCT/US2013/036802 2013.04.16

(56)对比文件

CN 1740941 A,2006.03.01,

(87)PCT国际申请的公布数据
W02013/169446 EN 2013.11.14

US 7734926 B2,2010.06.08,

CN 101627627 A,2010.01.13,

(73)专利权人 高通股份有限公司
地址 美国加利福尼亚州

CN 1581010 A,2005.02.16,

US 2009083856 A1,2009.03.26,

(72)发明人 苏迪普·拉维·科蒂林加尔
加里·阿瑟·钱贝拉

审查员 张述照

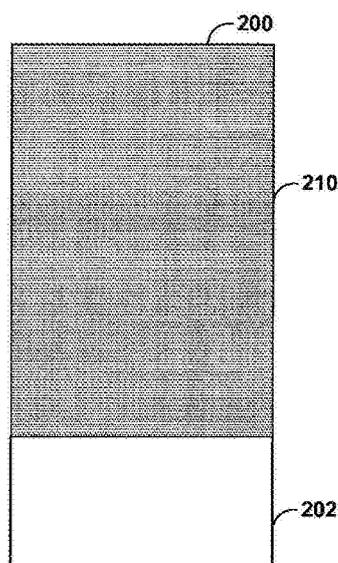
权利要求书5页 说明书18页 附图21页

(54)发明名称

硬件强制执行的输出安全设定

(57)摘要

本发明的方面一般是针对复制保护技术。可保护存储器中的区域以在所述存储器中建立未经授权的客户不能存取的安全存储区域。可接收解码存储在所述安全存储区域中的视频内容的请求。如果待解码的所述视频内容存储在所述安全存储区域中,则与所述硬件解码器相关联的第一MMU可强制执行所述视频内容将被解码成所述安全存储区域中的一或多个输出缓冲器的规则。可接收显示存储在所述安全存储区域中的所述经解码视频内容的请求。如果所述经解码视频内容存储在所述安全存储区域中,则与硬件显示处理器相关联的第二MMU可强制执行在所述硬件显示处理器与输出装置之间建立安全链路的规则。



1. 一种内容保护方法,其包括:

通过计算装置的硬件防火墙来保护计算装置中的存储器中的区域,以通过强制执行针对安全存储区域的读取和写入规则而在所述存储器中建立未经授权客户不能存取的安全存储区域;

接收解码存储在所述安全存储区域中的视频内容的请求;

如果待解码的所述视频内容存储在所述安全存储区域中,则通过与所述计算装置的硬件视频解码器相关联的第一存储器管理单元MMU强制执行规则,所述规则为所述视频内容将被解码成所述安全存储区域中的一或多个输出缓冲器,包含通过所述硬件视频解码器将所述视频内容解码成所述安全存储区域中的所述一或多个输出缓冲器;

接收显示存储在所述安全存储区域中的经解码视频内容的请求;以及

如果经解码视频内容存储在所述安全存储区域中,则通过与硬件显示处理器相关联的第二MMU强制执行规则,所述规则为在所述硬件显示处理器与输出装置之间建立安全链路,包含通过所述计算装置中的所述硬件显示处理器经由所述安全链路在所述输出装置处呈现经解码视频内容。

2. 根据权利要求1所述的方法,其中解码所述视频内容进一步包括:

通过所述第一MMU从所述硬件视频解码器中的客户端接收存取存储在所述安全存储区域中的所述视频内容的请求以及与所述请求相关联的客户端流识别符cSID;

通过所述第一MMU至少部分地基于所述cSID从多个上下文库中选择一上下文库;以及

使用经选定上下文库,将包含在所述请求中的虚拟地址翻译成所述安全存储区域内的物理地址。

3. 根据权利要求2所述的方法,其进一步包括:

通过与所述硬件视频解码器相关联的硬件安全块将与所述请求相关联的流识别符SID与SID安全寄存器进行比较,所述SID安全寄存器表示所述硬件安全块辨识为源自安全上下文的一组SID;以及

如果所述SID与所述SID安全寄存器中的多个SID之一匹配,则将所述SID的最高有效位设定为“1”,且将所述SID设定为所述cSID,且发出CPI位=“1”,其中所述CPI位指示事务是否来自内容保护代理。

4. 根据权利要求3所述的方法,其进一步包括:

使用所述CPI位编索引到所述第一MMU中的安全状态确定表中,以确定所述请求是否源自安全上下文,以及

使用所述cSID和所述CPI位编索引到所述第一MMU中的流匹配表中,以确定所述请求的所述上下文库。

5. 根据权利要求4所述的方法,其进一步包括:

在未授权所述请求存取所述安全存储区域的情况下,通过所述第一MMU返回页错误。

6. 根据权利要求1所述的方法,其中呈现经解码视频内容进一步包括:

通过所述第二MMU从所述硬件显示处理器中的客户端接收存取经解码视频内容的请求以及与所述请求相关联的客户端流识别符cSID;

至少部分地基于所述cSID从所述多个上下文库中选择所述上下文库;以及

使用经选定上下文库,将包含在所述请求中的虚拟地址翻译成所述安全存储区域内的

物理地址。

7. 根据权利要求6所述的方法,其进一步包括:

如果所述请求包含读取请求,则通过所述硬件显示处理器的显示处理器驱动器将所述cSID的最高有效位设定为“1”,且如果所述读取请求为安全,则发出CPI位=“1”,其中所述CPI位指示事务是否来自内容保护代理;以及

如果所述请求包含来自所述硬件显示处理器的一或多个客户端的写入请求,则通过所述硬件显示处理器将所述cSID的所述最高有效位设定为“1”,且在所述一或多个客户端中的任一者均受内容保护的情况下,发出所述CPI位=“1”。

8. 根据权利要求7所述的方法,其进一步包括:

使用所述CPI位编索引到所述第二MMU中的安全状态确定表中,以确定所述请求是否源自安全上下文,以及

使用所述cSID和所述CPI位编索引到所述第二MMU中的流匹配表中,以确定所述请求的所述上下文库。

9. 根据权利要求8所述的方法,其进一步包括:

在未授权所述请求存取所述安全存储区域的情况下,通过所述第二MMU返回页错误。

10. 一种内容保护设备,其包括:

存储器,其分区成非安全存储区域和安全存储区域;

硬件防火墙,其经配置以通过对所述安全存储区域强制执行读取和写入规则来防止对所述安全存储区域的未经授权存取;

硬件视频解码器,其经配置以接收解码存储在所述安全存储区域中的视频内容且将所述视频内容解码成所述安全存储区域中的一或多个输出缓冲器的请求;

第一存储器管理单元MMU,其与所述硬件视频解码器相关联,其中所述第一MMU经配置以强制执行所述视频内容将被解码成所述安全存储区域中的所述一或多个输出缓冲器的规则;

硬件显示处理器,其经配置以接收呈现经解码视频内容且经由安全链路在输出装置处呈现经解码视频内容的请求;以及

第二MMU,其与所述硬件显示处理器相关联,其中所述第二MMU经配置以强制执行在所述硬件显示处理器与所述输出装置之间建立安全链路的规则。

11. 根据权利要求10所述的内容保护设备,其中所述第一MMU进一步经配置以:

从所述硬件视频解码器中的客户端接收存取存储在所述安全存储区域中的所述视频内容的请求以及与所述请求相关联的客户端流识别符cSID;

至少部分地基于所述cSID从多个上下文库中选择上下文库;以及

使用经选定上下文库,将包含在所述请求中的虚拟地址翻译成所述安全存储区域内的物理地址。

12. 根据权利要求11所述的内容保护设备,其进一步包括:

硬件安全块,其与所述硬件视频解码器相关联,且经配置以将与所述请求相关联的流识别符SID与SID安全寄存器进行比较,所述SID安全寄存器表示所述硬件安全块辨识为源自安全上下文的一组SID;且如果所述SID与所述SID安全寄存器中的多个SID之一匹配,则将所述SID的最高有效位设定为“1”,将所述SID设定为所述cSID,且发出CPI位=“1”,其中

所述CPI位指示事务是否来自内容保护代理。

13. 根据权利要求12所述的内容保护设备,其中所述第一MMU进一步经配置以:

使用所述CPI位编索引到所述第一MMU中的安全状态确定表中,以确定所述请求是否源自安全上下文,以及

使用所述cSID和所述CPI位编索引到所述第一MMU中的流匹配表中,以确定所述请求的所述上下文库。

14. 根据权利要求13所述的内容保护设备,其中所述第一MMU进一步经配置以在未授权所述请求存取所述安全存储区域的情况下返回页错误。

15. 根据权利要求10所述的内容保护设备,其中所述第二MMU进一步经配置以:

从所述硬件显示处理器中的客户端接收存取经解码视频内容的请求以及与所述请求相关联的客户端流识别符cSID;

至少部分地基于所述cSID从所述多个上下文库中选择所述上下文库;以及

使用经选定上下文库,将包含在所述请求中的虚拟地址选择为所述安全存储区域内的物理地址。

16. 根据权利要求15所述的内容保护设备,其进一步包括:

显示处理器驱动器,其用于所述硬件显示处理器,所述显示处理器驱动器经配置以在所述请求包含读取请求的情况下,将所述cSID的最高有效位设定为“1”,且在所述读取请求安全的情况下,发出CPI位=“1”;且

在所述请求包含来自所述硬件显示处理器的一或多个客户端的写入请求的情况下,将所述cSID的所述最高有效位设定为“1”,且在所述一或多个客户端中的任一者均受内容保护的情况下,发出CPI位=“1”,其中所述CPI位指示事务是否来自内容保护代理。

17. 根据权利要求16所述的内容保护设备,其中所述第二MMU进一步经配置以:

使用所述CPI位编索引到所述第二MMU中的安全状态确定表中,以确定所述请求是否源自安全上下文,以及

使用所述cSID和所述CPI位编索引到所述第二MMU中的流匹配表中,以确定所述请求的所述上下文库。

18. 根据权利要求17所述的内容保护设备,其中所述第二MMU进一步经配置以在未授权所述请求存取所述安全存储区域的情况下返回页错误。

19. 一种内容保护设备,其包括:

用于保护计算装置中的存储器中的区域以通过强制执行针对安全存储区域的读取和写入规则在所述存储器中建立未经授权客户不能存取的所述安全存储区域的装置;

用于接收解码存储在所述安全存储区域中的视频内容的请求的装置;

如果待解码的所述视频内容存储在所述安全存储区域中,则用于强制执行所述视频内容将被解码成所述安全存储区域中的一或多个输出缓冲器的规则的装置,包含用于将所述视频内容解码成所述安全存储区域中的所述一或多个输出缓冲器的装置;

用于接收显示存储在所述安全存储区域中的经解码视频内容的请求的装置;以及

如果经解码视频内容存储在所述安全存储区域中,则用于强制执行建立到输出装置的安全链路的规则的装置,包含用于经由所述安全链路在所述输出装置处呈现经解码视频内容的装置。

20. 根据权利要求19所述的设备,其中所述用于强制执行所述视频内容将被解码成所述安全存储区域中的一或多个输出缓冲器的所述规则的装置进一步包括:

用于接收存取存储在所述安全存储区域中的所述视频内容的请求以及与所述请求相关联的客户端流识别符cSID的装置;

用于至少部分地基于所述cSID从多个上下文库中选择上下文库的装置;以及

用于使用经选定上下文库将包含在所述请求中的虚拟地址翻译成所述安全存储区域内的物理地址的装置。

21. 根据权利要求20所述的设备,其进一步包括:

用于将与所述请求相关联的第一流识别符SID与SID安全寄存器进行比较的装置,所述SID安全寄存器表示所述硬件安全块标识为源自安全上下文的一组SID;以及

如果所述SID与所述SID安全寄存器中的多个SID之一匹配,则用于将所述SID的最高有效位设定为“1”且将所述SID设定为所述cSID且发出CPI位=“1”的装置,其中所述CPI位指示事务是否来自内容保护代理。

22. 根据权利要求21所述的设备,其进一步包括:

用于使用所述CPI位编索引到安全状态确定表中以确定所述请求是否源自安全上下文的装置,以及

用于使用所述cSID和所述CPI位编索引到流匹配表中以确定所述请求的所述上下文库的装置。

23. 根据权利要求22所述的设备,其进一步包括:

用于在未授权所述请求存取所述安全存储区域的情况下返回页错误的装置。

24. 根据权利要求19所述的设备,其中用于强制执行所述视频内容将被解码成所述安全存储区域中的一或多个输出缓冲器的所述规则的装置进一步包括:

用于接收存取经解码视频内容的请求以及与所述请求相关联的客户端流识别符cSID的装置;

用于至少部分地基于所述cSID从所述多个上下文库中选择所述上下文库的装置;以及

用于使用经选定上下文库将包含在所述请求中的虚拟地址翻译成所述安全存储区域内的物理地址的装置。

25. 根据权利要求24所述的设备,其进一步包括:

如果所述请求包含读取请求,则用于将所述cSID的最高有效位设定为“1”且在所述读取请求安全的情况下发出CPI位=“1”的装置;以及

如果所述请求包含来自一或多个客户端的写入请求,则用于将所述cSID的所述最高有效位设定为“1”且在所述一或多个客户端中的任一者均受内容保护的情况下发出所述CPI位=“1”的装置,其中所述CPI位指示事务是否来自内容保护代理。

26. 根据权利要求25所述的设备,其进一步包括:

用于使用所述CPI位编索引到安全状态确定表中以确定所述请求是否源自安全上下文的装置,以及

用于使用所述cSID和所述CPI位编索引到流匹配表中以确定所述请求的所述上下文库的装置。

27. 根据权利要求25所述的设备,其进一步包括:

用于在未授权所述请求存取所述安全存储区域的情况下返回页错误的装置。

硬件强制执行的输出安全设定

[0001] 本申请案主张2012年5月10日申请的第61/645,577号美国临时申请案的权益,所述申请案的整个内容特此以引用的方式并入本文中。

技术领域

[0002] 本发明涉及内容处理,且更明确地说,涉及受复制保护的内容的处理。

背景技术

[0003] 复制保护解决方案可用来约束对受复制保护的内容的存取权。举例来说,复制保护解决方案可限制受复制保护的内容的未经授权重放或复制。流氓用户可能绕过复制保护解决方案,使得其可容易地复制和重放受复制保护的内容。

发明内容

[0004] 一般来说,本发明描述用于强制执行复制保护且防止使用硬件对受复制保护的内容的未经授权存取。当前软件复制保护解决方案在开源操作系统(例如,Android®操作系统)中可容易地被绕过。即使结合开源操作系统使用,基于硬件的复制保护解决方案也可能较难绕过。本文所描述的技术可包含端对端内容保护技术,其解决例如视频等媒体正在计算装置内部行进时的攻击。所述技术还可包含强制执行使用规则,且调整输入与输出之间的事务,以确保满足所有使用规则。所述技术还可包含强制执行各种内容保护机制的稳健性规则和顺从规则。

[0005] 在一个实例中,一种方法包含通过计算装置的硬件防火墙来保护计算装置中的存储器中的区域,以通过强制执行针对安全存储区域的读取和写入规则,建立存储器中不可由未经授权客户存取的安全存储区域。所述方法进一步包含接收对存储在安全存储区域中的视频内容进行解码的请求。所述方法进一步包含:如果待解码的视频内容存储在安全存储区域中,那么通过与计算装置的硬件视频解码器相关联的第一存储器管理单元(MMU)强制执行视频内容将解码成安全存储区域中的一或多个输出缓冲器的规则,包含通过硬件视频解码器将视频内容解码成安全存储区域中的一或多个输出缓冲器。所述方法进一步包含接收对显示存储在安全存储区域中的经解码视频内容的请求。所述方法进一步包含:如果经解码视频内容存储在安全存储区域中,那么通过与硬件显示处理器相关联的第二MMU强制执行在硬件显示处理器与输出装置之间建立安全链路的规则,包含通过计算装置中的硬件显示处理器经由安全链路在输出装置处呈现经解码视频内容。

[0006] 在另一实例中,一种内容保护设备包含存储器,其分区成非安全存储区域和安全存储区域。所述设备进一步包含硬件防火墙,其经配置以通过强制执行针对安全存储区域的读取和写入规则,来防止对安全存储区域的未经授权存取。所述设备进一步包含硬件视频解码器,其经配置以接收解码存储在安全存储区域中的视频内容且将所述视频内容解码成安全存储区域中的一或多个输出缓冲器的请求。所述设备进一步包含与硬件视频解码器相关联的第一存储器管理单元(MMU),其中所述第一MMU经配置以强制执行视频内容将被解

码成安全存储区域中的一或多个输出缓冲器的规则。所述设备进一步包含硬件显示处理器,其经配置以接收呈现所述经解码视频内容且经由安全链路在输出装置处呈现经解码视频内容的请求。所述设备进一步包含与硬件显示处理器相关联的第二MMU,其中所述第二MMU经配置以强制执行在硬件显示处理器与输出装置之间建立安全链路的规则。

[0007] 在另一实例中,一种设备包含用于保护计算装置中的存储器中的区域以通过强制执行针对安全存储区域的读取和写入规则建立存储器中不可由未经授权客户存取的安全存储区域的装置。所述设备进一步包含用于接收对存储在安全存储区域中的视频内容进行解码的请求的装置。所述设备进一步包含:如果待解码的视频内容存储在安全存储区域中,那么用于强制执行视频内容将被解码成安全存储区域中的一或多个输出缓冲器的规则的装置,包含用于将所述视频内容解码成安全存储区域中的一或多个输出缓冲器的装置。所述设备进一步包含用于接收显示存储在安全存储区域中的经解码视频内容的请求的装置。所述设备进一步包含:如果经解码视频内容存储在安全存储区域中,那么用于强制执行建立到输出装置的安全链路的规则的装置,包含用于经由安全链路在输出装置处呈现经解码视频内容的装置。

[0008] 在附图及下文描述中陈述一或多个实例的细节。将从描述和图式且从所附权利要求书明白其它特征、目标和优点。

附图说明

[0009] 图1A是说明根据本发明的方面的经配置以接收、处理和输出内容的计算系统的框图。

[0010] 图1B是说明根据本发明的方面的经配置以输出受复制保护内容的计算系统的框图。

[0011] 图2A和2B是说明根据本发明的方面将存储器划分为受复制保护区域和不受复制保护区域的框图。

[0012] 图2C是说明根据本发明的方面初始化和使用存储器的流程图。

[0013] 图2D是说明根据本发明的方面初始化和使用存储器的流程图。

[0014] 图3A是说明用于复制保护的解码器和显示处理器的初始化的流程图。

[0015] 图3B是说明具有内容保护的受复制保护重放的调用的流程图。

[0016] 图4A是说明根据本发明的方面的存储器管理单元(MMU)的框图。

[0017] 图4B是说明根据本发明的方面的替代存储器管理单元(MMU)的框图。

[0018] 图5是说明根据本发明的方面的由存储器管理单元用来存取存储器的上下文库的框图。

[0019] 图6A是说明根据本发明的方面的视频解码器的框图。

[0020] 图6B是说明根据本发明的方面的由安全块执行的过程的流程图。

[0021] 图7A到7C是说明根据本发明的方面的显示处理器108的框图。

[0022] 图8A是说明根据本发明的方面的借助于显示处理器接收读取请求的过程的流程图。

[0023] 图8B是说明根据本发明的方面的借助于显示处理器接收写入请求的过程的流程图。

[0024] 图8C是说明根据本发明的方面的由显示处理器的存储器管理单元用来存取存储器的上下文库的框图。

[0025] 图9是说明根据本发明的方面的用于确定是否允许将受复制保护的内容显示到HDMI装置上的硬件逻辑的框图。

[0026] 图10是说明根据本发明的方面的传输流包处理器的框图。

[0027] 图11是说明根据本发明的方面的传输流结构和数据的框图。

[0028] 图12是说明根据本发明实施例的用于解码和显示受复制保护的视频内容的方法的流程图。

具体实施方式

[0029] 图1是说明根据本发明的方面的经配置以接收、处理和输出内容的计算系统的框图。如图1A中所示,计算装置100A可接收内容,例如视频输入152,可处理接收到的内容,且可输出经处理的内容,例如视频输出154。计算装置100A可接收受保护内容以及不受保护的内容。在一些实例中,受保护内容可为只能由计算装置100的经授权用户和/或组件存取的内容,且因此所述内容应受保护,计算装置100A的未经授权的用户和/或组件无法存取所述内容。

[0030] 计算装置100A可在内容受保护区150中处理受保护的内容,且可在自由内容区170中处理不受保护的内容,包含并行处理受保护和不受保护的内容。内容受保护区150可包含受保护缓冲器,其为受保护内容提供存储器隔离。内容区150可保护内容,计算装置100A的未经授权的用户和/或组件无法存取所述内容,使得仅经授权组件可被允许存取所述受保护内容。相反,自由内容区170可包含计算装置100A的不提供此存储器隔离和保护的组件。内容受保护区150和自由内容区170可并行处理内容,使得内容受保护区150可处理受保护内容,且在自由内容区170处理不受保护内容时,使受保护内容与计算装置100A的不是内容受保护区150的部分的组件隔离。

[0031] 内容受保护区150可强制执行安全要求,以保护受保护内容。对于经压缩位流的保护,内容受保护区150可强制执行以下要求:仅在用于输出经解密受保护内容的存储器位置只能由计算装置100A的安全组件(例如,总线的安全总线主控器)存取的情况下,允许解密经加密受保护内容的任何企图。内容受保护区150还可强制执行以下要求:计算装置100A的处理经解密受保护内容的组件具有防止在内容受保护区150的外部写入内容的机制。内容受保护区150还可强制执行以下要求:用于信任区(TrustZone)系统的相同存取控制方案在从任何DRM来源解密的经压缩位流上使用。对于未经压缩位流的保护,内容保护区150可强制执行以下要求,涉及安全内容的任何变换将产生安全输出。内容保护区150还可对输出装置施加额外要求,例如如果将内容输出到HDMI链路,那么强制执行 HDCP。

[0032] 内容受保护区150可与内容保护模块通信耦合,例如链路保护模块162、数字权利管理(DRM)模块164、内容保护中心函数(CPCF)模块166、条件存取系统(CAS)模块168、存储保护模块170等。链路保护模块162可经配置以保护点对点连接中的内容传递,其中发射器验证接收器,且可经配置以在受保护内容进入和退出内容受保护区150时保护受保护内容。链路保护模块162的实例可包含高带宽数字内容保护(HDCP)和经由因特网协议的数字传输内容保护(DTCP-IP)。DRM模块164可经配置以实现受保护内容的云管理,以便要求客户在云

中验证其本身,以接收用于存取受保护内容的密钥。CPFC模块166可包含管理进入和退出接口的软件,且可强制执行用于确定哪些组件被授权存取受保护内容的规则。CAS模块168可为用于广播TV以保护其服务的机制。CAS模块168的实例可包含用于ISDB-T的Multi2、用于DVB的DVB-CI+,以及用于有线卫星的其它专有CAS系统,以及IPTV。

[0033] 内容受保护区150可对到内容受保护区150中的输入和来自内容受保护区150的输出施加要求。输入到内容受保护区150的要求可包含:要求使用内容受保护区150的任何应用程序将其内容复制到内容受保护区150中;要求在使用所支持的解密协议的密码模块中执行解密;要求对经解密缓冲器(即,用于密码模块的输出缓冲器)的地址的控制由信任区或硬件约束管理,以强制执行内容受保护区150地址范围;以及如果HDCP有效,则要求捕获HDMI输入的视频捕获将限制到内容受保护区150的存储区域的内容传递。对来自内容受保护区150的输出的要求可包含:要求来自内容受保护区150的内容仅可用于选择硬件(例如,编解码器和显示硬件)且选择软件(例如,密码模块和信任区);以及要求通过密码模块将受保护内容递送到内容受保护区150外部。

[0034] 图1B是说明根据本发明的方面的经配置以输出受复制保护内容(例如受复制保护的媒体(例如,音频、图像和视频))的计算系统的框图。如图1B中所示,计算装置100B可包含存储器102、密码模块104、视频解码器106、硬件防火墙107、显示处理器108、传输流包处理器(TSP)110、信任区114、操作系统116、视频解码器驱动器118、显示处理器驱动器120和应用程序122。在一些实例,计算装置可由一或多个集成电路组成,例如芯片上系统、一或多个微处理器、一或多个微处理器核等。在一些实例中,计算装置100B可类似于图1A中所示的计算装置100A,且在一些实例中,计算装置100B的组件(例如,存储器102、密码模块104、视频解码器106、硬件防火墙107、显示处理器108、TSP110、信任区114、操作系统116、视频解码器驱动器118、显示处理器120和/或应用程序122中的一或多者)可用来保护如图1A中所示的内容受保护区150内的受保护内容。

[0035] 受复制保护的内容可存储在存储器102中。应用程序122可将解密受复制保护内容的请求发送到密码模块104。信任区114和硬件防火墙107可确保密码模块104的输出只可由例如视频解码器106和显示处理器108等安全硬件组件读取,且密码模块104可将受复制保护内容解密到存储器102的受复制保护区域中。在一些实例中,信任区114可包含CPFC模块166。TSP110可强制执行内容保护规则,以确保TSP110所处理的每个传输流包均遵循一组复制保护规则。视频解码器106可从存储器102的受复制保护区域读取经解密内容,解码所述经解密内容,且将经解码内容存储在存储器102的受复制保护区域中。显示处理器108可存取存储器102的受复制保护区域中的经解码内容,且可将所述内容呈现到显示器上。

[0036] 操作系统116可为高级操作系统(HLOS),例如Android®、iOS®、Linux®、Unix®、Windows®等。显示处理器驱动器120可为使其它软件能够与显示处理器108通信的软件。视频解码器驱动器118可为使其它软件能够与视频解码器106通信的软件。信任区114可为软件和/或硬件的组合。在一些实例中,信任区114可包含安全核心,其与同一处理器核上的操作系统116同时执行,且包含供操作系统116与安全核心通信的驱动器。信任区114可使用安全性扩展来保护其自身,使其免于在操作系统116中运行的代码,使得甚至已经设法获得操作系统116中的完整管理员特权的攻击者也无法获得对信任区114的存取权。

[0037] 可通过保护存储器102的只能被信任硬件和/或软件存取以存取存储在存储器102

的受保护区域中的受复制保护内容的区域,来将存储器102划分成安全区域和非安全区域。图2A和2B是说明根据本发明的方面将存储器200(其可类似于图1B中所示的存储器102)划分成安全和非安全区域的框图。如图2A中所示,存储器200的选择性部分可由信任区114和操作系统116保护,使得存储器200可划分成非安全存储区域210和安全存储区域202,使得仅某些信任硬件和/或软件被允许存取存储在安全存储区域202中的受复制保护内容。安全存储区域202可为存储器200的较大连续区域,例如存储器200的可划分成四个千字节页的五十兆字节区域。保护安全存储区域202可包含通过硬件防火墙107,设定和强制执行安全存储区域202上的存取控制规则,使得未经授权的客户不能够存取安全存储区域202。一般来说,包含存储器200的计算装置(例如图1A中所示的计算装置100A或图1B中所示的计算装置100B)的受信任组件可强制执行以下规则:如果用于所述组件的输入缓冲器在安全存储区域中,那么用于所述组件的输出缓冲器必须也在安全存储区域中。

[0038] 如图2B中所示,代替于保留存储器的较大连续区域来用于存储受复制保护内容,存储器200的较小区域可作为用于存储受复制保护内容的安全存储区域204由信任区114和操作系统116动态地分配和保护。举例来说,安全存储区域204可为存储器200的1兆字节区域,其可经1兆字节和4千字节分页。可根据需要分配额外安全存储区域204,且还可将安全存储区域204去分配和返还给存储器102,以供在不再需要时,用作非安全存储区域200。硬件防火墙107可控制对安全存储区域204的存取,使得未经授权的客户不能够存取安全存储区域204。

[0039] 图2C是说明根据本发明的方面的存储器的安全存储区域的按需初始化和使用(例如图2B中所示)的过程的流程图。如图2C中所示,可以较小的块(例如,一兆字节块)分配安全存储区域。如果以存储器的一兆字节块分配安全存储区域,那么可在冷启动时初始化存储器200,且可清空跟踪存储器200的安全和非安全存储区域的存取管理表(AMT)。在一些实例中,AMT可为允许存储器的一个兆字节块受存取保护的硬件。在热启动时,信任区114可清空标记为AMT中的安全存储区域的存储区域的存储器内容。图1B中所示的高级操作系统(HLOS)(例如操作系统116)可将存储器的一块保留作为安全区域(250)。在分配存储器的每一安全存储区域后,例如如果以存储器的一兆字节块分配安全存储区域,那么可从HLOS(高级操作系统,例如操作系统116)核心分配一兆字节连续块的列表。一旦分配所述存储器,就可将指向安全存储区域的指针传递到信任区114。信任区114可检查所述指针的一兆字节对准,且将所述存储器映射在存储器102内(252),可清空安全存储区域的存储器内容(254),且可将AMT中的对应旗标翻转为对于对应于所讨论的存储器的所述一兆字节块的位置来说为真(256)。信任区114可向HLOS发送安全存储区域的分配为完整的指示(258)。一旦针对安全存储区域的复制保护使用情况结束,HLOS就可向信任区114发送释放安全存储区域的请求,使得可从所述安全存储区域去分配所述存储器,且可将其重新填充在HLOS核心内。信任区114可检查一兆字节对准指针(262),清空安全存储区域的内容(264),且可将AMT中的对应旗标翻转为对于所讨论的存储器的所述一兆字节块的位置为假(266)。信任区114可向HLOS发送安全存储区域已释放用于一般存储器用途的指示(268)。

[0040] 图2D是说明根据本发明的方面的预切开存储器102(例如图2A中所示)的初始化和使用的框图。如图2D中所示,HLOS核心或HLOS启动过程中的安全驱动器可作出锁定一条存储器以用于复制保护使用的明确请求(270)。HLOS可将陷阱发送到信任区114,以请求在经

锁定的所述条存储器内保留存储器以用于复制保护(272)。信任区114可检查所保留的存储器的物理地址的范围(274)。信任区114还可清空所保留存储器的现存内容(276)。信任区114可进一步经由硬件防火墙107添加存取保护,使得仅安全客户(例如,具有适当的CP_VMID、HV_VMID或APROT_NS=0的客户)可存取所保留的存储器(278)。为了释放存储器,信任区114可清空所保留存储器的内容,且可释放硬件防火墙107所提供的存取保护。信任区114可向HLOS发送所保留的存储器已被分配的指示(280)。在不再使用所保留的存储器之后,HLOS可将释放所保留的存储器的请求发送到信任区114(282)。响应于接收到释放所保留存储器的请求,信任区114可检查所保留存储器的物理地址的范围(284),清空所保留存储器的存储器内容(286),且可将存取保护从所保留存储器移除,例如通过调整硬件防火墙107的规则以使所保留存储器编程为可由HLOS_VMID存取(288)。信任区114可向HLOS发送所保留存储器的释放完成的指示(290)。

[0041] 图3A是说明用于复制保护的解码器106和显示处理器108的初始化的流程图。如图3中所示,视频解码器驱动器118(其可正在HLOS(例如,操作系统116)中运行)在首次启动时通过将陷阱发送到信任区114以起始视频解码器106来请求视频解码器106的初始化(302)。信任区114可通过初始化和存取保护视频解码器106的安全块(包含设置安全地址空间)来响应所述陷阱(304)。还可执行视频解码器106的相关联存储器管理(MMU)配置。视频解码器106的MMU可用复制保护固件页表来初始化,可设置上下文库和缓冲器,且可验证和加载视频解码器固件(306)。视频解码器106可在复位之后就绪。显示处理器驱动器120可向信任区114发送启动显示处理器108的请求(308)。信任区114可用页表和缓冲器来设置显示处理器的上下文库,可启动显示处理器108,且可为显示处理器108启用安全性(310)。

[0042] 图3B是说明具有内容保护的受复制保护重放的调用的流程图。如图3B中所示,受复制保护应用程序(例如,图1B中所示的应用程序122)可向信任区114发送解密受复制保护内容(例如,受复制保护视频)的请求(312)。作为响应,信任区114可确定用于经解密内容的输出缓冲器是否受硬件防火墙107保护,且可使密码模块104能够解密受复制保护内容。密码模块104可解密受复制保护内容,且输出存储器(由硬件防火墙107保护以防止来自未经授权客户的未经授权存取的存储器)的受保护区域中的输出缓冲器中的经解密内容。

[0043] 信任区114可将解密已完成报告回给应用程序122(314)。作为响应,应用程序122可向视频解码器驱动器118发送对视频解码器106解码存储在存储器102的安全存储区域中的经解密内容的请求(316)。视频解码器106可解码所述内容的标头,估计需要含有经解密内容的输出缓冲器的大小,且可经由视频解码器驱动器118将所估计输出缓冲器的量映射到存储器102的安全存储区域(318)。

[0044] 一旦用于视频解码器106的输出缓冲器已成功映射到存储器102中,视频解码器驱动器118就可使视频解码器106能够解码所述内容的帧,且将经解码内容输出到存储器102的安全存储区域中的输出缓冲器中(320)。

[0045] 当视频解码器106结束解码内容帧时,可通知视频解码器驱动器118(322)。接着,视频解码器驱动器118可通知应用程序122视频解码器106已完成解码内容帧(324)。应用程序122可通知显示处理器驱动器120经解码的内容准备好供显示处理器108呈现到显示器上(326)。显示处理器驱动器120可将存储器102的安全存储区域的下伏页映射到显示处理器108的专用于受复制保护内容的上下文库中(328)。显示处理器108可将存储器102的安全存

储区域中的经解码内容帧呈现到显示器 (330)。如果显示器为HDMI显示器,那么显示处理器108可确定在将经解码内容帧输出到HDMI显示器之前是否启用HDCP。

[0046] 图4A是说明根据本发明的方面的存储器管理单元的框图。计算装置的组件(例如,图1B中所示的计算装置100B的视频解码器106和显示处理器108)可包含或以其它方式利用存储器管理单元(MMU)来翻译请求且存取存储器,例如图2A中所示的安全存储区域202,或图2B中所示的安全存储区域204。如图4A中所示,处理器400可对应于图1B中所示的视频解码器106或显示处理器108,或可对应于利用本发明的技术的另一系统的不同处理器。处理器400可包含多媒体核402,例如视频解码器核或显示处理器核,以及MMU406。多媒体核402可与MMU406通信,例如经由高级微控制器总线架构(AMBA),以经由存储器接口(例如,AMBA高级可扩展接口(AXI))与存储器(例如,存储器102)事务。MMU406可包含安全状态确定(SSD)表408和流匹配表410。

[0047] 多媒体核402可在安全模式和非安全模式下操作。如果多媒体核402在安全模式下操作,那么可将CP_IND设定为1。如果多媒体核402在非安全模式下操作,那么可将CP_IND位设定为0。流ID(SID)还可与来自多媒体核402的事务相关联。多媒体核402可通过将SID的最高有效位设定为CP_IND来产生客户SID(cSID)。作为事务的一部分,多媒体核402可将CP_IND位和cSID传送到MMU406。

[0048] SSD表408可接收事务的CPI作为输入,且可确定所述事务是否安全。SSD表408可输出所述事务的非安全(NS)状态,其中NS状态0指示事务是安全的,且能够在系统总线上断言APROTNS=安全,而NS状态1指示事务是非安全的,且只能在系统总线上断言APROTNS=非安全。流匹配表410可将来自多媒体核402的事务的相关联cSID以及由SSD表408输出的指示事务是否安全的NS状态确定视为输入,且可输出所述事务的初始上下文412。如下文相对于图5所论述,初始上下文412可由MMU406用来使用上下文存取存储器102。

[0049] 图4B是说明根据本发明的方面的替代存储器管理单元(MMU)的框图。如图4B中所示,处理器450可对应于图1B中所示的视频解码器106或显示处理器108,或可对应于利用本发明的技术的另一系统的不同处理器。处理器450可包含多媒体核452,例如视频解码器核或显示处理器核,以及MMU456。多媒体核452可与MMU456通信,例如经由高级微控制器总线架构(AMBA),以经由存储器接口(例如,AMBA高级可扩展接口(AXI))与存储器(例如,存储器102)事务。MMU456可包含安全状态确定(SSD)表458和流匹配表(SMT)450。

[0050] SMT450可分成安全和非安全SMT,而MMU456还可包含安全部分462和非安全部分464。CInst信号可指示来自核的指令获取,且可将此信号传播到上下文选择和页选择逻辑。使用来自客户端口的CInst位=1来存取时的页中的XN位可升高异常。

[0051] 可使用CPI位(其又指向SMT460)来驱动每一事务的安全状态。用于SMT460的安全部分的流匹配逻辑可由信任区114控制,而用于SMT460的非安全部分的流匹配逻辑可由通用软件控制。

[0052] 图5是说明根据本发明的方面的由存储器管理单元用来存取存储器的上下文库的框图。上下文库可充当页表以将虚拟地址请求翻译成存储器中的物理地址,例如图1B中所示的存储器102的物理地址。如图5中所示,MMU,例如图4A中所示的MMU406,可使用三个上下文库:CB0 502、CB1 504和CB2 506。CB0 502可经配置以存储在受复制保护地址范围之外的存储器,CB1 504可经配置以存取在受复制保护地址范围内的存储器,且CB2 506可经配

置以存取在受复制保护地址范围内的固件存储器区。上下文库502、504和506可包含翻译逻辑和/或映射以充当页表,且将虚拟地址请求翻译成存储器(例如,存储器102)中的物理地址。源自中央处理单元客户端(其SID的最初两个最高有效位可设定为“1”)的事务可对应于流匹配表410中选择CB2 506的仅有条目。来自其cSID的最高有效位设定为“1”的客户端的事务可对应于流匹配表410中选择CB1 504的条目,且来自其cSID的最高有效位处于“0”的客户端的事务可对应于流匹配表410中选择CB0 502的条目。以此方式,对受复制保护地址范围的存取可限于安全客户端和安全事务。举例来说,图4A中的MMU406可使用上下文库504来基于MMU406所产生的初始上下文412翻译来自多媒体核402的虚拟地址。表1为说明以下表中所说明的流匹配表410的条目的示范性表:

[0053] 表1

[0054]

子客户端	cSID	事务域状态	存储器存取	CB 映射
非安全 ARM9 数据	0b00000000	非内容保护	非内容保护存取	CB0
VSP_CMDIF	0b00000001	非内容保护	非内容保护存取	CB0
VSP_AP	0b00000010	非内容保护	非内容保护存取	CB0
VSP_SP_SG	0b00000011	非内容保护	非内容保护存取	CB0
VSP_CPU_DMA	0b00000100	非内容保护	非内容保护存取	CB0
VPP	0b00000101	非内容保护	非内容保护存取	CB0
CP ARM9 数据	0b10000000	内容保护	内容保护存取	CB1
CP VSP_CMDIF	0b10000001	内容保护	内容保护存取	CB1
CP VSP_AP	0b10000010	内容保护	内容保护存取	CB1
CP VSP_SP_SG	0b10000011	内容保护	内容保护存取	CB1
CP VSP_CPU_DMA	0b10000100	内容保护	内容保护存取	CB1
CP VPP	0b10000101	内容保护	内容保护存取	CB1

[0055]

安全 FW ARM9 数据	0b11000000	受保护 FW 中的数 据存取	内容保护 ARM9 图像 存取	CB2
安全 FW ARM9 指令	0b11000110	受保护 FW 中的指 令存取	内容保护 ARM9 图像 存取	CB2

[0056] 图6A是说明根据本发明的方面的视频解码器的框图。如图6A中所示,视频解码器600可对应于图1B中所示的视频解码器106,或可对应于利用本发明的技术的另一系统的不同视频解码器。视频解码器600可包含存储器管理单元(MMU)子系统602,其由视频解码器固件编程以强制执行关于受复制保护内容的安全性规则。视频解码器600还可包含硬件防火墙610,其对视频解码器600中的寄存器空间强制执行存取控制规则,以防范对那些寄存器空间的外部存取。视频解码器600还可包含处理器子系统608和视频编解码器子系统612,其可用来决定内容。MMU子系统602所强制执行的实例安全性规则可包含:只有视频解码器600的输入和输出缓冲器两者均属于安全存储区域(例如,图2A和2B中所示的安全存储区域202或204)的受复制保护地址范围内时,视频解码器600所处理的受复制保护内容才可保持安全且在受保护会话中受到保护。如果例如视频解码器600的输出缓冲器不属于安全存储区域的地址范围内,那么MMU子系统602可终止受保护会话,且可发送违规通知。

[0057] MMU子系统602可包含MMU606,例如图1中所示的MMU406,以及安全块604。视频解码

器固件和信任区114对安全块604进行编程和查询。安全块604可包含CPA开始和CPA结束寄存器,其表示存储器中的安全存储区域的受内容保护虚拟地址范围,MMU子系统602可用其来确定输入或输出缓冲器是否属于所述范围内。安全块604还可包含FW开始和FW结束寄存器,其表示在受内容保护虚拟地址范围内的安全固件虚拟地址范围,其表示存储视频解码器600的视频解码器固件的虚拟地址范围。安全块604还可包含SID安全寄存器,其表示安全块604辨识为正在受保护(即,源自内容保护上下文)的流ID(SID)的集合。SID可与通过总线发射到视频解码器600的客户端和/或客户端请求/事务相关联。如果客户端或事务与安全块604辨识为正受保护的SID相关联,那么允许客户端或事务存取受内容保护的存储器。以下表2中列举所述寄存器:

[0058] 表2

[0059]

寄存器	用途	复位值
SEC_SID_0_SECURE SEC_SID_1_SECURE SEC_SID_2_SECURE SEC_SID_3_SECURE SEC_SID_4_SECURE SEC_SID_5_SECURE	这组寄存器表示所述组SID,其中SEC_SID_X_SECURE表示SID=X。寄存器值“1”指示对应的SID受保护,且可存取CPA范围内的受内容保护的存储器。寄存器值“0”指示SID不受保护,且只能被准许存取CPA范围之外的不受保护的存储器。	0x00000000(所有寄存器)
SEC_CPA_START	安全虚拟地址范围的开始地址。CPA范围包含FW图像区。	0x00000000
SEC_CPA_END	安全虚拟地址范围的结束地址。CPA范围包含FW图像区。	0x00000000
SEC_FW_START	安全FW虚拟地址范围的开始地址	0x00000000
SEC_FW_END	安全FW虚拟地址范围的结束地址	0x00000000

[0060] 图6B是说明根据本发明的方面的可由安全块执行的过程的流程图。如图6B中所示,安全块604可执行确定视频解码器600所接收到的请求是否源自内容保护上下文(即,来自被允许存取受保护存储器的客户端)的过程。安全块604可确定事务是否源自处理器客户端(例如,源自视频解码器600的处理器子系统608)(652)。如果事务确实源自处理器客户端,如果事务正存取的地址在受内容保护的虚拟地址范围内,那么安全块604可将此事务的SID的最高有效位设定为“1”,且如果事务正存取的地址在固件虚拟地址范围内,那么可将此事务的SID的第二最高有效位设定为“1”(654)。将SID的最高有效位设定为“1”可指示允许事务选择受复制保护的上下文库(下文所论述)。

[0061] 如果事务并未源自处理器客户端,那么安全块604可确定事务的安全寄存器(例如,上文的表中的SEC_SID_X_SECURE寄存器中的一者)是否设定为1(656)。如果将事务的安全寄存器设定为1,那么安全块604可将事务的SID的最高有效位设定为“1”,且可针对此事务发出CPI=1(658)。如果事务的安全寄存器不设定为1,那么安全块604可将事务的SID的最高有效位设定为“0”,且可针对此事务发出CPI=0(660)。CPI=1可为事务来自内容保护代理的指示,而CPI=0可为事务不来自内容保护代理的指示。

[0062] 图7A到7C是说明根据本发明的方面的显示处理器的实例的框图。如图7A和7B中所示,显示处理器700可对应于图1B中所示的显示处理器108,或可对应于利用本发明的技术的另一系统的不同显示处理器。显示处理器700可包含MMU子系统702和移动显示处理器

(MDP) 708。MMU子系统702可包含安全块704和MMU706，例如图4A中所示的MMU406。显示处理器700可包含存取保护单元 (APU2)，其保护寄存器，例如寄存器712和714。MMU子系统702还可包含寄存器保护单元 (RPU) 718，其保护MMU子系统702中的某些寄存器，例如受保护寄存器716，而例如寄存器714等其它寄存器可保持不受保护。显示处理器700可包含存取保护单元 (APU)，以保护显示处理器108免于未经授权的存取。

[0063] 类似于图4A中所示的视频解码器600的MMU子系统602，MMU706可强制执行关于受复制保护内容的安全性规则。MMU706可从显示处理器700中的MDP客户端接收对经由总线（例如AXI总线）来自存储器的数据的请求，且所述总线可经由相关联的cSID信号指示所述请求是否来自受复制保护的上下文，其中cSID信号中的低（例如，“0”）最高有效位指示不受内容保护的存取，而cSID信号的高（例如，“1”）最高有效位指示受内容保护的存取。MDP708可有责任来驱动cSID信号的最高有效位。对于每个客户端的每个存取请求，可检查所述存取以确定存储器存取是否安全。MDP708可依靠软件（例如，图1B中所示的显示处理器驱动器120）以编程存取的状态和/或类型），且可适当地断言相关联cSID信号的最高有效位。如上文相对于图5所论述，断言相关联cSID的最高有效位对于存取正确的上下文库以将与存取请求相关联的虚拟地址翻译成物理地址来说是重要的。MMU706可经由AXI存储器接口722基于存取请求存取存储器（例如，图1B中所示的存储器102）。MDP708可经由AHB编程总线722将视频内容传送到输出发射模块724，使得输出发射模块724可在输出装置726处呈现视频内容。

[0064] 如图7C中所示，MDP708的多个客户端可连接到MMU706以从存储器读取且写入到存储器，例如图1B中所示的存储器102。所述客户端可由MMU706合并成单个AXI。可将所述客户端分组为写入到存储器102的写入客户端750以及从存储器读取的读取客户端752。

[0065] 读取客户端752可包含rgb1、rgb2和rgb3；vig1、vig2和vig3；dma0和dma1以及光标客户端。写入客户端750可包含：

[0066] wb0：为旋转路径或线回写路径回写；

[0067] wb1：为实现所要性能所必需的旋转路径或线回写路径回写，因为MDP708可支持非常高的分辨率；以及

[0068] wb2：回写路径以支持无线显示或同时回写功能性。

[0069] 写入客户端750和读取客户端752可用一般客户端接口协议来存取MMU706以从存储器102请求数据，且这些存取可由MMU706翻译成AXI请求。AXI接口可提供支持以经由cSID信号指示对存储器的受保护存取。MMU706可从客户端接收内容保护信息。因此，MDP708可负责正确地驱动cSID的最高有效位，使得其在AXI端口上反映。因此，对于MDP708的客户端所进行的每次获取，可检查请求以确定存储器存取是否安全。

[0070] 图8A是说明根据本发明的方面的接收显示处理器（例如图7A中所示的显示处理器700或图1B中所示的显示处理器108）的读取请求的过程的流程图。如图8A中所示，显示处理器驱动器（例如图1B中所示的显示处理器驱动器120）可为读取请求编程SW_STATUS寄存器以指示读取请求的内容保护状态。MDP708可读取所述寄存器，且如果SW_STATUS寄存器指示所述读取请求受内容保护，那么将相关联cSID信号的最高有效位设定为“1”，且可将CPI信号设定为“1”。相反，如果SW_STATUS寄存器指示所述读取请求不受内容保护，那么MDP708可将相关联cSID信号的最高有效位设定为“0”，且可将CPI信号设定为“0”。SW_STATUS寄存器

不受硬件防火墙保护,且可在一般显示处理器寄存器空间中。

[0071] 图8B是说明根据本发明的方面的接收显示处理器(例如图7A中所示的显示处理器700或图1B中所示的显示处理器108)的写入请求的过程的流程图。如图8B中所示,MDP708可确定是否任何客户端均受内容保护。如果是,那么MDP708可将相关联cSID信号的最高有效位设定为“1”,且可将CPI信号设定为“1”。相反,如果客户端中无一者受内容保护,那么MDP708可将相关联cSID信号的最高有效位设定为“0”,且可将CPI信号设定为“0”。

[0072] 图8C是说明根据本发明的方面的显示处理器的MMU(例如图7A中所示的MMU706)用来存取存储器的上下文库的框图。如图8C中所示,显示处理器(例如,图7A中所示的显示处理器700或图1B中所示的显示处理器108)可使用两个存储器库:CB0和CB1。CB0可映射到不受内容保护存储器存取,且CB1可映射到受内容保护的存储器存取,例如表3中所示:

[0073] 表3

[0074]

客户端	cSID	事务域状态	存储器存取	CB映射
所有客户端	0b0xxxx	非内容保护	非内容保护存取	CB0
所有客户端	0b1xxxx	内容保护	内容保护存取	CB1

[0075] 一旦选择上下文库,MMU706就可尝试将所述请求的虚拟地址翻译成存储器中的物理地址。如果翻译成功,那么准予对存储器的存取权。否则,可发生页错误。表4展示这些不同虚拟地址翻译情形:

[0076] 表4

[0077]

cSID	经MMU翻译	结果
NCP	否	页错误。
NCP	是	不受内容保护的存取。
CP	否	页错误。
CP	是	受内容保护的存取。

[0078] 如上文所述,可使用SW_STATUS寄存器来确定读取请求的内容保护状态。然而,SW_STATUS寄存器不受硬件防火墙保护,且可在一般显示处理器寄存器空间中。尽管SW_STATU寄存器不受硬件防火墙保护,但以下表5说明MMU706可如何处置对显示处理器寄存器的存取:

[0079] 表5

[0080]

输入缓冲器状态	SW 状态	输出状态	HW CP 状态	结果/评论
CP	NCP	CP	NCP	输入将被阻挡在 MDP 之外，因为当其尝试存取归因于不一致性而将违反所述存取的 CP 缓冲器时，MDP HW 将指示 NCP 存取。 由于输出状态为 CP，向存储器的写出将不成功，但硬件将驱动 NCP 存取。所述存取将导致页错误。
CP	NCP	NCP	NCP	输入将被阻挡在 MDP 之外，因为当其将尝试存取归因于不一致性而将违反所述存取且导致页错误的 CP 缓冲器时，MDP HW 将指示 NCP 存取。 由于输出状态为 NCP，向存储器的写出将成功，且硬件将驱动 NCP 存取。所述数据将不为真内容，而是已返回到 MDP 的任何内容。
CP	CP	NCP	CP	读取数据将成功，因为 MDP HW 将指示有效的对 CP 空间的 CP 存取。 输出将不成功，因为 MDP 硬件将驱动对将导致页错误的对 NCP 空间的 CP 存取。
CP	CP	CP	CP	读取数据将成功，因为 MDP HW 将指示有效的对 CP 空间的 CP 存取。 写出也将成功，因为 MDP 硬件将驱动对 CP 空间的 CP 存取。
NCP	CP	NCP	CP	输入将被阻挡在 MDP 之外，因为当其将尝试存取归因于不一致性而将违反所述存取且导致页错误的 CP 缓冲器时，MDP HW 将指示 CP 存取。 输出将不成功，因为 MDP 硬件将驱动对将导致页错误的对 NCP 空间的 CP 存取。
NCP	CP	CP	CP	输入将被阻挡在 MDP 之外，因为当其将尝试存取归因于不一致性而将违反所述存取且导致页错误的

[0081]

				NCP 缓冲器时，MDP HW 将指示 CP 存取。 输出将成功，因为 MDP 硬件将驱动对 CP 空间的 CP 存取。然而，所述数据将为返回到 MDP 的任何内容。
NCP	NCP	CP	NCP	读取数据将成功，因为 MDP HW 将指示有效的对 NCP 空间的 NCP 存取。 输出将不成功，因为 MDP 硬件将驱动对将导致页错误的对 CP 空间的 NCP 存取。
NCP	NCP	NCP	NCP	读取数据将成功，因为 MDP HW 将指示有效的对 NCP 空间的 NCP 存取。 输出将成功，因为 MDP 硬件将驱动对 NCP 空间的 NCP 存取。

[0082] 输入缓冲器状态——如信任区114所知晓且编程的输入缓冲器的状态。

[0083] SW状态——如由显示处理器驱动器120编程的安全性状态/类型，且MDP708用其来产生到MMU706的客户端侧上的cSID的最高有效位。

[0084] 输出状态——如由信任区114编程的输出缓冲器的状态。

[0085] CP-指示内容保护。

[0086] NCP-指示非内容保护。

[0087] 因此,导致成功完成的仅有有效条件可包含一切均受复制保护的的条件,或一些均不受复制保护的的条件,且即使SW_STATUS寄存器不受硬件保护,安全性在显示处理器700中也不受危害。

[0088] 如果受复制保护的内容将被驱动到高清晰度多媒体接口(HDMI)装置,那么可强制执行要求启用高带宽数字复制保护(HDCP)的要求。显示处理器(例如图1B中所示的显示处理器108)可包含适当地处置此情形的硬件。图9是说明根据本发明的方面的用于确定是否允许将受复制保护的内容显示到HDMI装置上的硬件逻辑的框图。如图9中所示,显示处理器可包含硬件逻辑900,其在受保护内容将输出的情况下、HDMI被选作输出接口的情况下以及不启用HDCP的情况下阻挡HDMI内容。

[0089] 图10是说明根据本发明的方面的传输流包处理器(TSPP)的框图。如图10中所示,TSPP1000(类似于图1B中所示的TSPP110)可包含TSPP安全存储器管理单元(SMMU)1002、内容保护区(CPZ)策略器1012、总线存取管理器(BAM)无数据路径(NDP)1010、TSPP输出级1008以及TSPP输入级1006。

[0090] TSPP1000可接收包括多媒体数据的传输流,且可处理接收到的传输流,例如通过解多路复用接收到的传输流,使得接收到的多媒体数据可由计算装置的其它组件(例如图1B中所示的计算装置100B,例如图1B中所示的视频解码器106和显示处理器108)处理。在TSPP初始化时,信任区114可配置TSPP1000,使得TSPP1000含有指示保护什么类型的内容的静态配置。

[0091] CPZ策略器1012可在硬件中强制执行内容保护规则,且确保TSPP1000所处理的每个传输流包的输出准许一组指定的规则。CPZ策略器1012可针对每一包写入计算是否允许输出。假如HLOS根据CPZ策略器1012规则配置了TSPP1000,数据路径将流式传输内容。如果HLOS软件尝试过攻击,那么CPZ策略器1012可丢弃所述内容,且TSPP1000可断言安全性违反中断。

[0092] BAM NDP1010可提供管理缓冲器和通知的硬件-软件接口。因为缓冲器管理是从HLOS执行,且因此可总是不受保护,因此停用CPI位。BAM NDP1010中的所有管均可共享同一SID。TSPP输出级1006可负责经由TSPP SMMU1002将数据写入到总线。TSPP输出级1006中的每一BAM生产者管可具有由信任区114配置有CPI位的单独上下文。CPI位启用的管上下文被视为安全的。每一上下文还可具有单独且固定的SID。TSPP输入级1008可负责经由TSPP SMMU1002读取输入缓冲器。TSPP输入级1008中的每一BAM消费者管可具有由信任区114配置CPI位的单独上下文。CPI位启用的消费者管上下文被视为安全的。每一上下文还可具有单独且固定的SID。

[0093] TSPP SMMU1002可包含安全状态确定表(SSDT)1014、流匹配表(SMT)1016,以及两个上下文库CB0 1018和CB1 1020。CB1 1020可为安全上下文库,且CB0 1018可为非安全上下文库。上下文库CB0 1018和CB1 1020在输出至总线时可映射到相关VMID。映射表可为固定的。SID将附加到CPI位,且映射到CB0 1018和CB1 1020。所有0x1xxxxx SID均可映射到安全上下文库CB1 1020,且所有0x0xxxxx SID均可映射到非安全上下文库CB0 1018。

[0094] 图11是说明根据本发明的方面的传输流结构和数据的框图。如图11中所示,MPEG-2传输流可包括若干基本流的多路复用,所述基本流各自具有其自己的包识别符(PID)。

MPEG-2传输流可为用于流式传输视频、音频和其它数据的一般容器,且广泛用于广播和流式传输系统(DVB、ATSC、IPTV、DLNA等)。

[0095] 基本流的多路复用内的每一流可为封包化基本流(PES)或区段流。可使用PES来流式传输视频、音频和副标题。可使用区段流来广播描述所述多路复用的程序和服务信息(PSI/SI)表。程序或服务可由若干流组成。举例来说,CNN广播可包括音频、视频、副标题和PSI/SI流。在同一多路复用中,ESPN和天空(Sky)广播也可与CNN广播包含在一起。

[0096] 传输流包可具有188字节的固定大小,其中至少4个字节为标头,且其与可为有效负载。为了保护对特定服务的存取,广播器可加密属于这些服务的传输流。传输流加密可在TS包等级下执行:当可加密有效负载时,包标头可总是不受阻碍。通常,可仅加密视频流。解密所述流且根据其使用规则保护器内容免受复制/存储/盗窃可为芯片集责任。

[0097] TSPP处理和流可由HLOS配置。此配置可包含输入、处理、输出格式和输出管。因为HLOS可能不被信任以配置保护内容保护区的路径,所以此间隙可由TSPP1000中的CPZ策略器1012填充。

[0098] TSPP1000可从连接到解调器或条件存取模块的物理传输流接口(TSIF)接收输入。此接口为非安全的,且经由其运载的数据受加密保护。TSPP1000还可经由非安全BAM管从RAM接收此输入。此使用情况可包含IPTV的风味,其在传输流等级下加密数据且加密个人视频记录器重放。

[0099] TSIF/NS管规则(表6中所示)

[0100] 表6

[0101]

输出格式	处理	流类型	生产者(输出)管保护强制执行	评论
原始	解密=否	不管	NS 管	包经加密或不受阻碍,且不需要存取保护
原始	解密=是 && 加密=否	不管	安全管	当输出原始包时,TSPP无法确定流格式(PES\区段)或类型(音频\视频\等)。必须假定包正运载视频,且需要受进一步保护。
原始	加密=是	不管	NS 管	经加密离开 TSPP 的任何内容必须受存取保护
PES	解密=否	不管	NS 管	包经加密或不受阻碍,且不需要存取保护
PES	解密=是	包含在受保护 PES 类型列表中	到受保护管的有效负载 标头可去往 NS 管	无
PES	解密=是	不包含在受保护 PES 类型列表中	到 NS 管的有效负载 标头可去往 NS 管	无

[0102] TSPP1000可提供对mpeg2解多路复用和解密的硬件加速。可存在其中不使用TSPP1000的解密能力,但仍可使用TSPP1000的解多路复用特征。

[0103] 这些使用情况的解密可在块模式下执行,且可将传输流视为任何位流。可将解密的输出馈入到TSPP1000中以用于解多路复用。由于所述内容不受阻碍,因此其可受存取保护,且可经过安全消费者管。

[0104] 对于非安全输入, 可仅加密所要基本流的传输流包(视频)。安全管可在同一安全性等级下处理整个传输流包。

[0105] 安全管规则(表7中所示)

[0106] 表7

[0107]

输出格式	处理	流类型	生产者(输出)管保护强制执行	评论
原始	加密=否	不管	安全管	原始包可运载受保护或不受保护的数据, 其可由 TSP110 确定。默认是保护
原始	加密=是	不管	NS 管	数据正受加密保护
PES	N/A	包含在受保护 PES 类型列表中	到受保护管的有效负载到 NS 管的标头	无
PES	N/A	不包含在受保护 PES 类型列表中	到 NS 管的有效负载到 NS 管的标头	无

[0108] 信任区114可在初始化时用在运行时期可不改变的以下信息来配置TSP110。

[0109] 流类型(流_id)可作为PES标头发射, 且在PES组合期间由TSP110剖析。配置至多达10个受保护PES类型可为可能的。每一PES类型可具有8位值和8位掩码。举例来说, 视频的PES类型可包含: 值:11100000掩码:11110000, DSC-CC将为值:11110010掩码:11111111。默认列表可仅包含视频: 值:11100000掩码:11110000

[0110] TSP110可允许配置至多达10个PID滤波器。每一滤波器可由值和掩码(类似于TSP110中的所有PID滤波器)组成。默认列表可包含PAT、NIT、CAT、TSDT, 其可分别在PID0、1和2中运载。信任区114可在信道开关处配置生产者和消费者管的CPI位。

[0111] 广播中间件软件可知晓根据程序映射表中的描述符加密哪些PID。当在解多路复用驱动器中选择那些PID时, 也可指定生产者管。HLOS软件可请求信任区114保护所述管。信任区114可启用CPI位以便锁定所述管。未能设定CPI位将导致安全性违反中断, 其可由TSP110中的CPZ策略器1012断言, 且可丢弃所述数据。在服务拆卸期间, HLOS软件可请求信任区114通过停用CPI位来解锁所述管。

[0112] 使用受保护消费者管(DLNA/CPRM/蓝光)的所有技术的中间件可请求信任区114通过启用CPI位来保护消费者管。未能设定CPI位可导致受保护内容的泄露。TSP110可将所述内容视为不受保护(由于无解密将在TSP110内部发生), 且可将输出路由到HLOS缓冲器。在拆卸期间, HLOS可要求信任区114通过停用CPI位来解锁消费者管。

[0113] 电视玩家可在HLOS中运行。电视玩家可管理从源节点(解多路复用)通过解码器到显示器的数据管。另外, 电视玩家还可处置时钟恢复(PCR)和A/V同步。

[0114] 需要经历解码和显示的每一视频帧可包封在单个PES包中。定时信息可包含在PES标头中, 且经压缩的帧可包含在PES有效负载中。可仅在有效负载上应用存取保护机制。

[0115] 由于管上下文表示单个缓冲器且使用单个MMU上下文库, 因此可能有必要在硬件中使PES标头与有效负载分开。可将每一视频流路由到两个不同管: 标头管和有效负载管。可将指向有效负载的指针附加到PES标头, 以容易地使标头关联到有效负载。

[0116] 如上文所述, 将所述流中的一些发送到安全缓冲器, 因为其运载的内容无法由

TSPP110确定。信任区114中的受保护解多路复用器可充当CPZ策略器1012的扩展。数据中的一些可到达信任区114,尽管其可能无意受保护(例如PSI区段)。信任区114可确定是否可将此不受保护的数据复制到将由HLOS使用的非安全缓冲器。

[0117] PES PID可由CPZ策略器1012处置,因此到安全解多路复用器的输入可为运载区段的原始传输流包。然而,因为可使用HLOS来命令TSPP110将PES PID的原始包发送到信任区114,所以安全解多路复用器可不能够依靠结构化为区段的内容的假定。相反,受保护的解多路复用器可检验内容结构化为区段的事实。

[0118] 为了确定安全解多路复用器正在将区段复制到非安全缓冲器,可首先成功地组合所述区段。成功组合可为一种情况,其中:1.经组合的区段大小等于标头中的区段大小;2.区段大小不大于4KB;且3.所计算的循环冗余校验(CRC)与曾发射的CRC匹配。组合本身可在安全缓冲器上执行。响应于组合正成功完成,可将经组合的区段复制到非安全缓冲器。

[0119] 可能存在其中区段中的一些应受保护而其它不应受保护的情形。举例来说,程序映射表(PMT)可永不受保护。然而,可保护运载交互式游戏的区段。因此,可能有必要具有安全解多路复用器正向HLOS暴露的较精细粒度。信任区114中的安全解多路复用器可配置有区段的保护等级:1.总是将区段发送到HLOS;2.永不将区段发送到HLOS;以及3.可发送到HLOS的表id的列表。

[0120] 假如TSPP110中的任何功能性需要软件回退,信任区114中的安全解多路复用器可处置所有安全性和/或受保护内容。实例可包含:1.PES类型辨识失效:所有经解密PES将发送到安全管。信任区114可剖析PES标头且确定类型。因此,其可将缓冲器复制到非安全缓冲器;以及2.PES组合失效:可将所有经解密传输流包放置在安全缓冲器中。安全解多路复用器可根据PES类型在适当缓冲器中组合PES。

[0121] SMMU映射表(表8):

[0122] 表8

[0123]

子客户端	cSID	存储器存取	CB映射
TSPP BAM NDP	0000000000	HLOS存取	CB0
TSPP管上下文	0xxxxxxxxxxx	HLOS存取	CB0
TSPP管上下文	1xxxxxxxxxxx	内容保护	CB1

[0124] 图12是说明根据本发明实施例的用于解码和显示受复制保护的视频内容的方法的流程图。如图12中所示,所述方法可包含通过计算装置100的硬件防火墙来保护计算装置100的存储器102中的区域,以通过对安全存储区域强制执行读取和写入规则在存储器102中建立不可由未经授权的客户端存取的安全存储区域(1202)。所述方法可进一步包含接收对存储在安全存储区域中的视频内容进行解码的请求(1204)。所述方法可进一步包含:如果待解码的视频内容存储在安全存储区域中,那么通过与计算装置100的硬件视频解码器106相关联的第一存储器管理单元(MMU)强制执行规则,所述规则为视频内容将解码成安全存储区域中的一或多个输出缓冲器,包含通过硬件视频解码器106将视频内容解码成安全存储区域中的一或多个输出缓冲器(1206)。所述方法可进一步包含显示存储在安全存储区域中的经解码视频内容的请求(1208)。所述方法可进一步包含:如果经解码视频内容存储在安全存储区域中,那么通过与硬件显示处理器108相关联的第二MMU强制执行规则,所述

规则为在硬件显示处理器108与输出装置之间建立安全链路,包含通过计算装置100中的硬件显示处理器108经由安全链路在输出装置处呈现经解码视频内容(1210)。

[0125] 在一些实例中,解码视频内容可进一步包含:通过从硬件视频解码器106中的客户端接收第一MMU存取存储在安全存储区域中的视频内容的请求以及与所述请求相关联的第一客户端流识别符(cSID);通过第一MMU至少部分地基于第一cSID从多个上下文库中选择一上下文库;以及使用选定上下文库将包含在请求中的虚拟地址翻译成安全存储区域内的物理地址。在一些实例中,所述方法可进一步包含通过与硬件视频解码器106相关联的硬件安全块将与所述请求相关联的第一SID与流识别符(SID)安全寄存器进行比较,所述SID安全寄存器表示安全性块标识为源自安全上下文的一组SID;以及如果SID与SID安全寄存器中的多个SID中的一者匹配,那么将SID的最高有效位设定为“1”,将SID设定为cSID,且发出CPI位=“1”。在一些实例中,所述方法可进一步包含使用CPI位编索引到第一MMU中的安全状态确定表中,以确定请求是否源自安全上下文;以及使用cSID和CPI位编索引到第一MMU中的流匹配表中,以确定所述请求的上下文库。在一些实例中,所述方法可进一步包含:如果未授权所述请求存取安全存储区域,那么通过第一MMU返回页错误。

[0126] 在一些实例中,呈现经解码视频内容可进一步包含:通过从硬件视频解码器108中的客户端接收第二MMU接收存取安全存储区域中的经解码视频内容的请求以及与所述请求相关联的客户端流识别符(cSID);至少部分地基于cSID从多个上下文库中选择上下文库;以及使用选定上下文库将包含在请求中的虚拟地址翻译成安全存储区域内的物理地址。

[0127] 所述方法可进一步包含:如果请求包含读取请求,那么通过硬件显示处理器的显示处理器驱动器将cSID的最高有效位设定为“1”,且如果读取请求为安全的,那么发出CPI位=“1”;以及如果所述请求包含来自硬件显示处理器的一或多个客户端的写入请求,那么通过硬件显示处理器将cSID的最高有效位设定为“1”,且在所述一或多个客户端中的任一者均受内容保护的情况下,发出CPI位=“1”。

[0128] 所述方法可进一步包含使用CPI位编索引到第二MMU中的安全状态确定表中,以确定请求是否源自安全上下文;以及使用cSID和CPI位编索引到第二MMU中的流匹配表中,以确定所述请求的上下文库。所述方法可进一步包含:如果未授权所述请求存取安全存储区域,那么通过第二MMU返回页错误。

[0129] 在一或多个实例中,所描述的功能可以硬件、软件、固件或其任何组合来实施。如果以软件来实施,那么所述功能可作为一或多个指令或代码存储在计算机可读媒体上,或经由计算机可读媒体传输。计算机可读媒体可包括计算机数据存储媒体或包括促进计算机程序从一处传递到另一处的任何媒体的通信媒体。数据存储媒体可为可由一或多个计算机或一或多个处理器存取以检索指令、代码和/或数据结构以供实施本发明中所描述的技术的任何可用媒体。作为实例而非限制,所述计算机可读媒体可包含RAM、ROM、EEPROM、CD-ROM或其它光盘存储装置、磁盘存储装置或其它磁性存储装置,或可用于运载或存储呈指令或数据结构形式的所要程序代码且可由计算机存取的任何其它媒体。同样,可恰当地将任何连接称作计算机可读媒体。举例来说,如果使用同轴电缆、光纤电缆、双绞线、数字订户线(DSL)或例如红外线、无线电及微波的无线技术从网站、服务器或其它远程源传输软件,那么同轴电缆、光纤电缆、双绞线、DSL或例如红外线、无线电及微波的无线技术包含于媒体的定义中。在本文中使用时,磁盘及光盘包含压缩光盘(CD)、激光光盘、光学光盘、数字多功能

光盘 (DVD)、软性磁盘及蓝光光盘,其中磁盘通常以磁性方式再现数据,而光盘使用激光以光学方式再现数据。上文的组合也应包含在计算机可读媒体的范围内。

[0130] 代码可由一或多个处理器执行,例如一或多个数字信号处理器 (DSP)、通用微处理器、专用集成电路 (ASIC)、现场可编程逻辑阵列 (FPGA),或其它等效集成或离散逻辑电路。因此,如本文中所使用的术语处理器可指上述结构或适合于实施本文中所描述的技术的任一其它结构中的任一者。另外,在一些方面中,本文所述的功能性可提供于经配置以用于编码和解码的专用硬件和/或软件模块内,或并入在组合式编解码器中。并且,可将所述技术完全实施于一或多个电路或逻辑元件中。

[0131] 本发明的技术可在各种各样的装置或设备中实施,包含无线手持机、集成电路 (IC) 或一组 IC (即,芯片组)。本发明中描述各种组件、模块或单元,以强调经配置以执行所揭示技术的装置的功能方面,但不一定要求由不同硬件单元来实现。相反,如上文所述,各种单元可组合在编解码器硬件单元中,或由互操作硬件单元的集合提供,包含如上文所述的一或多个处理器,结合合适的软件和/或固件。

[0132] 本发明还包含附加的附件,其形成本发明的一部分,且明确地并入本文中。

[0133] 已描述了各种实例。这些和其它实例在所附权利要求书的范围内。

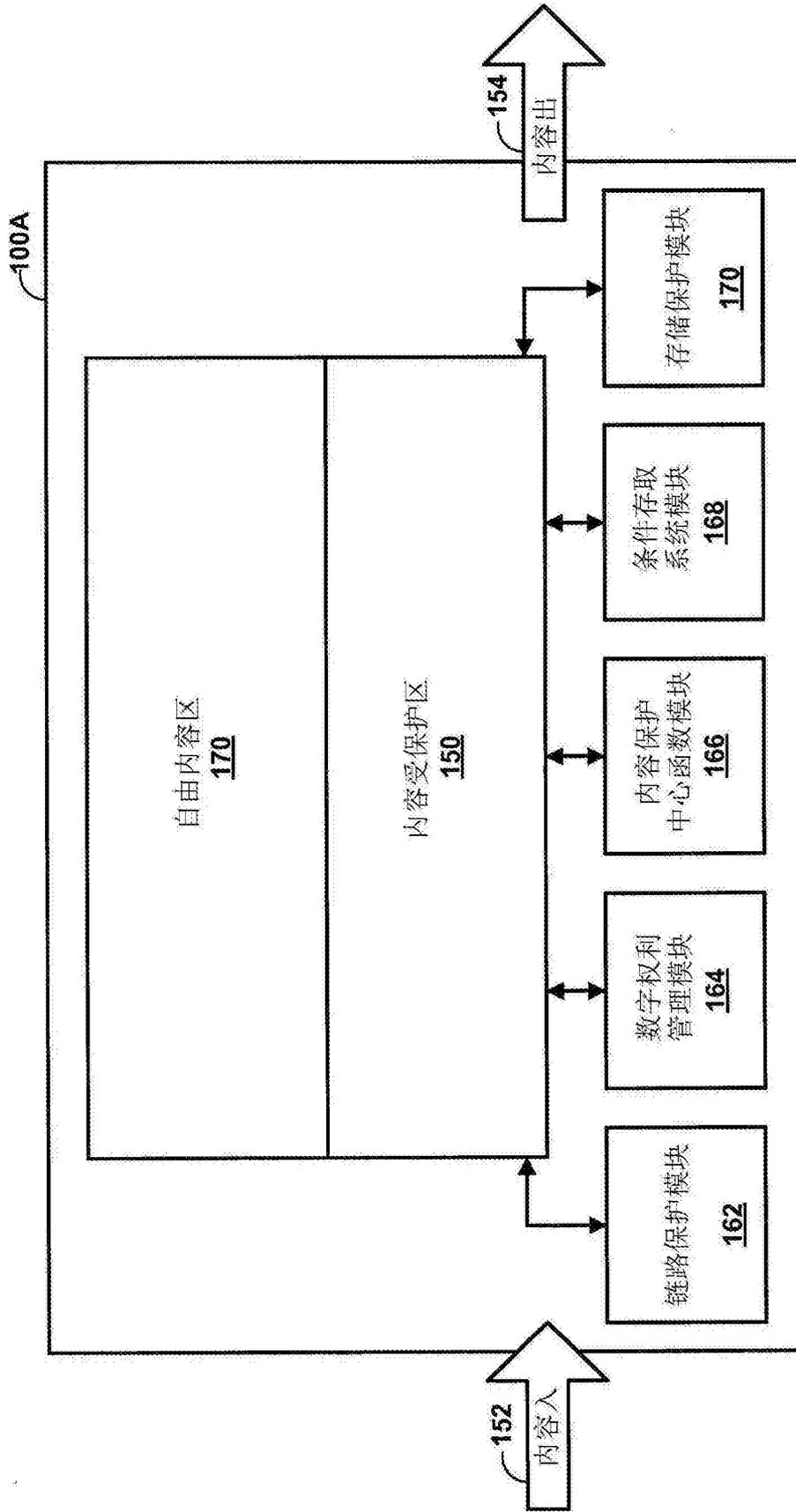


图1A

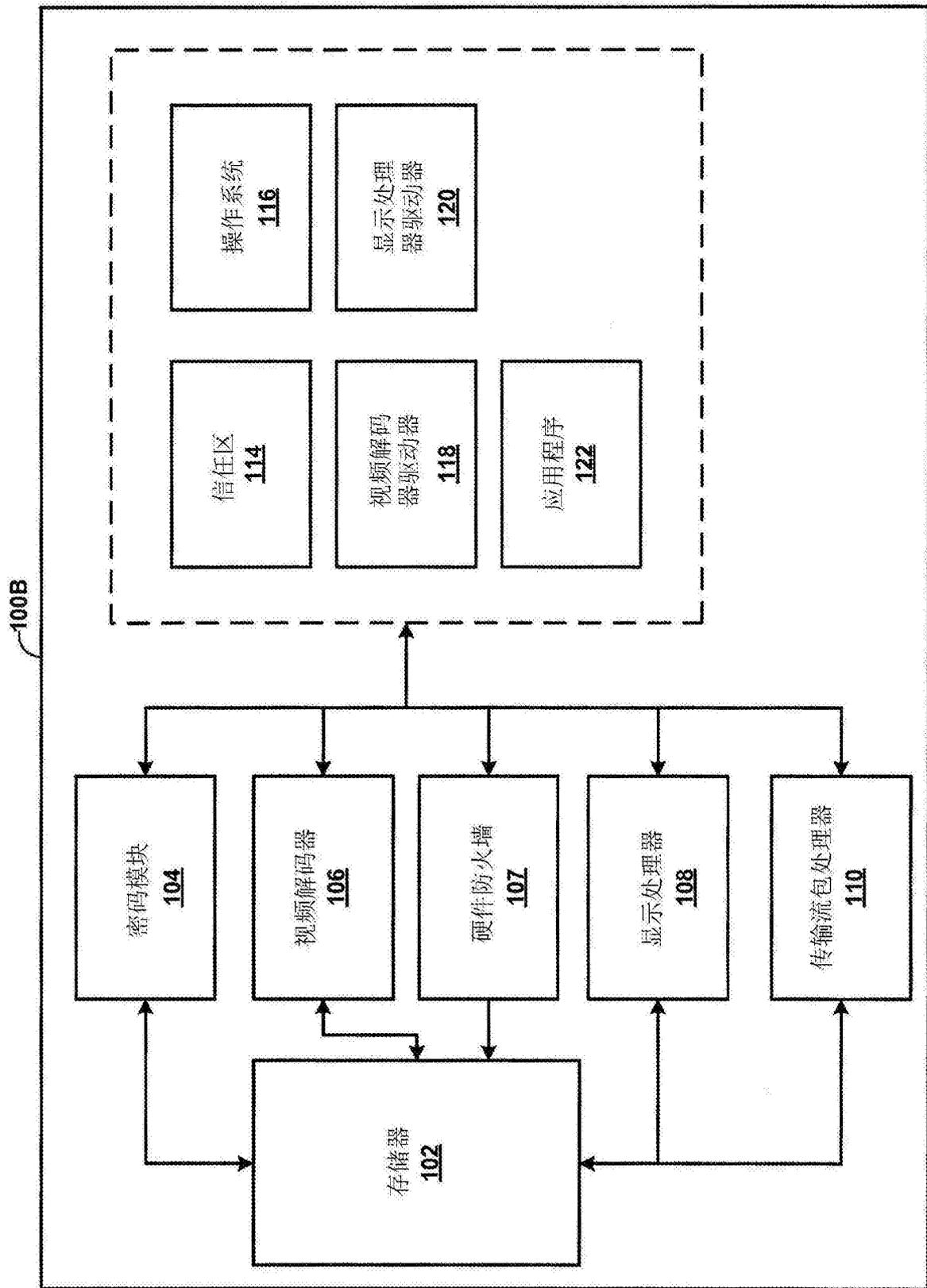


图1B

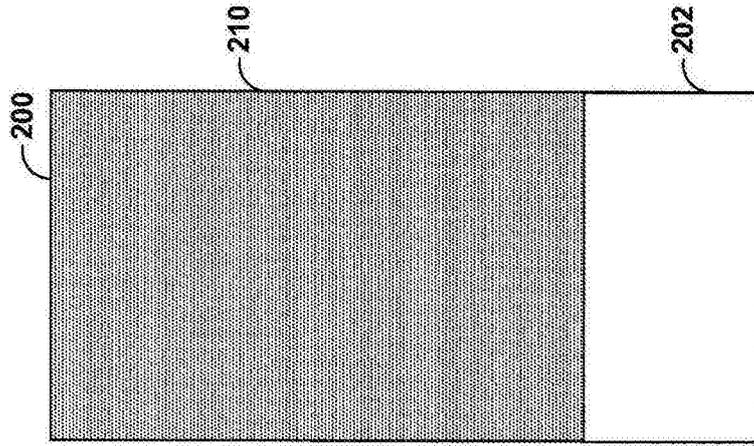


图2A

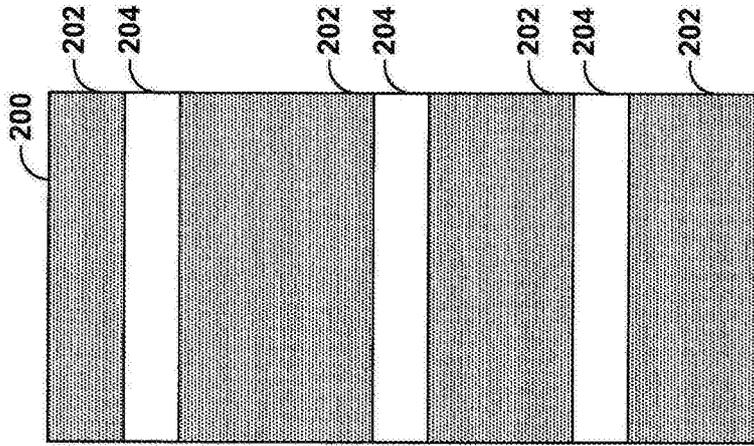


图2B

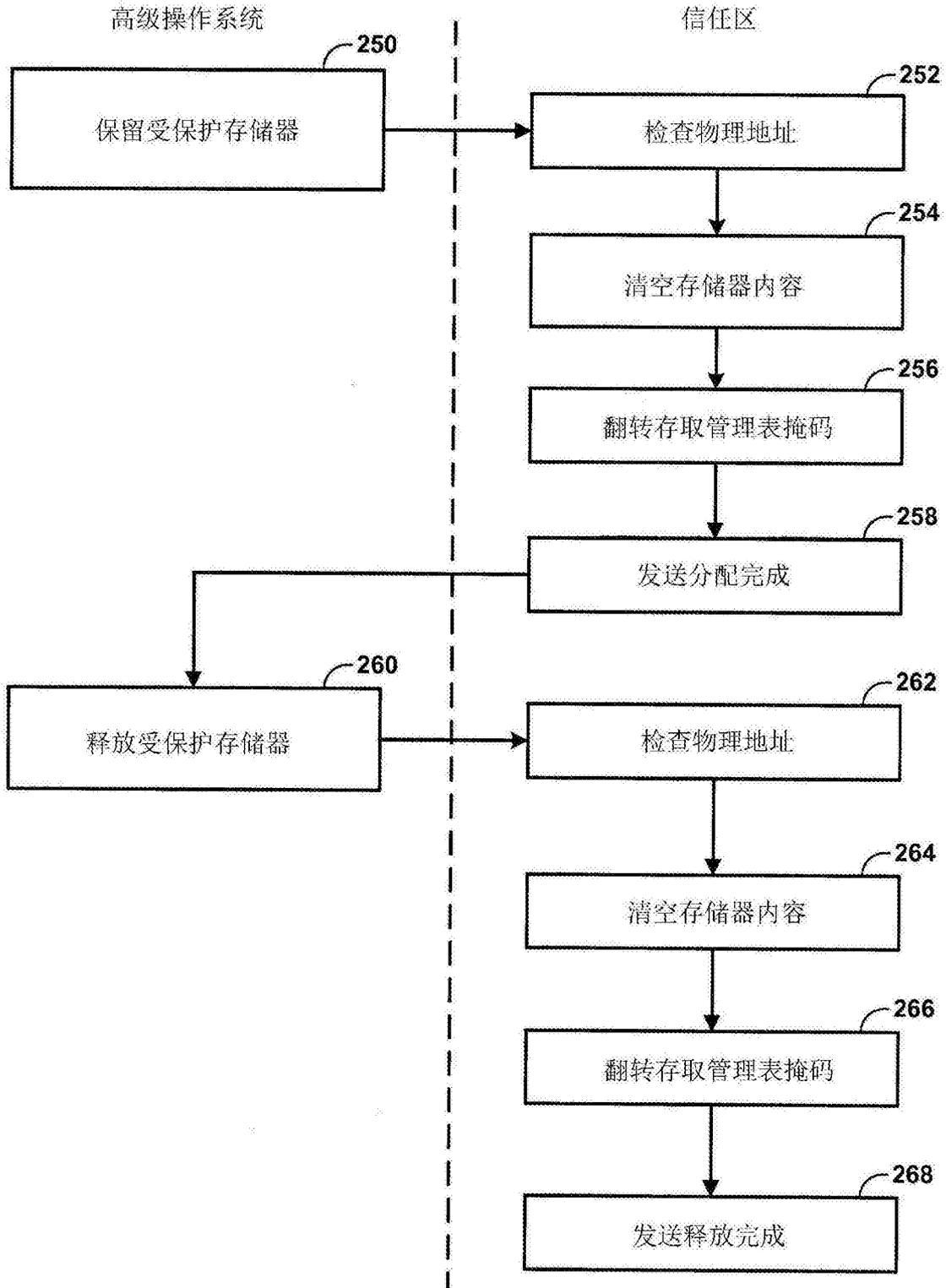


图2C

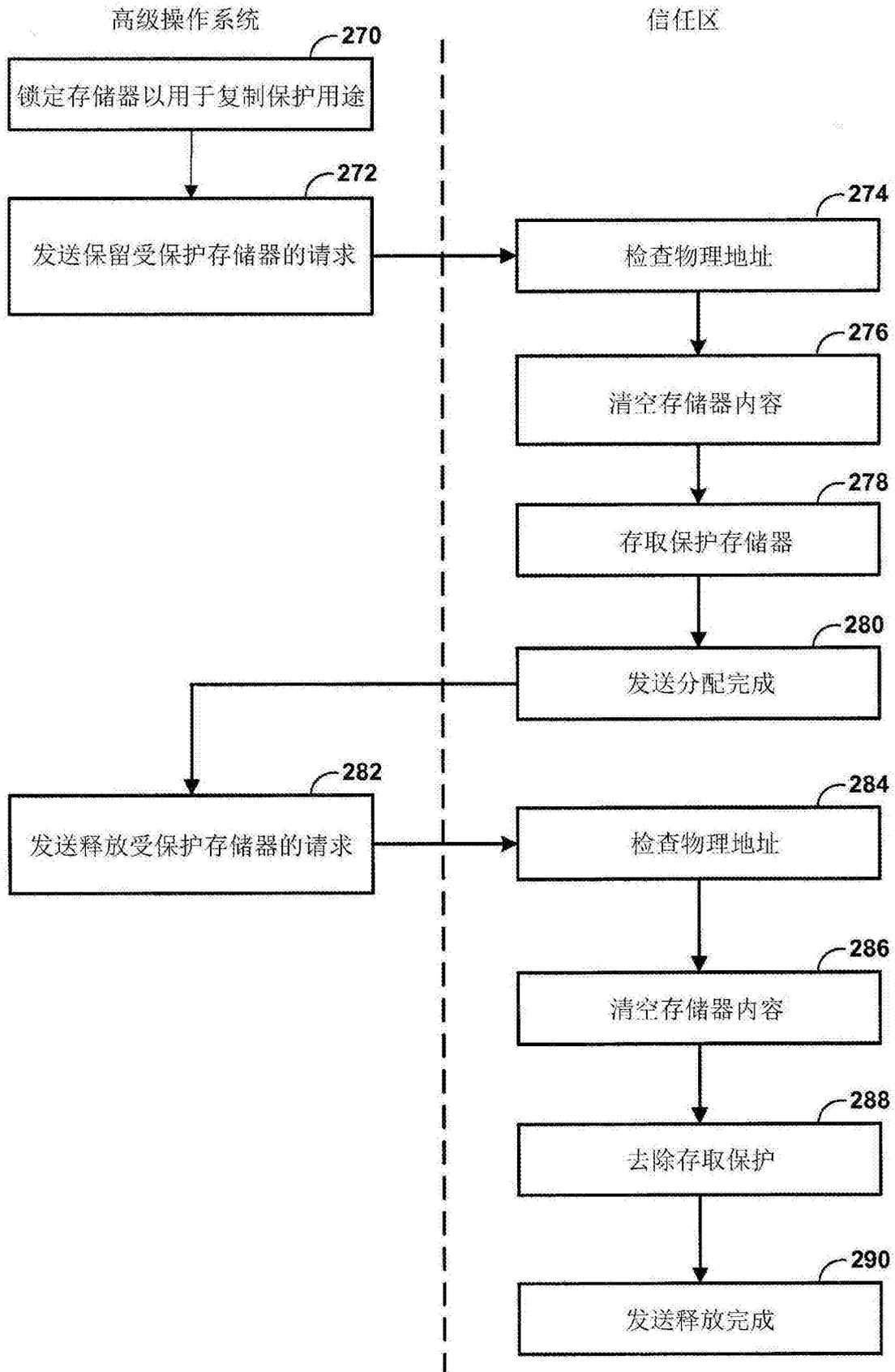


图2D

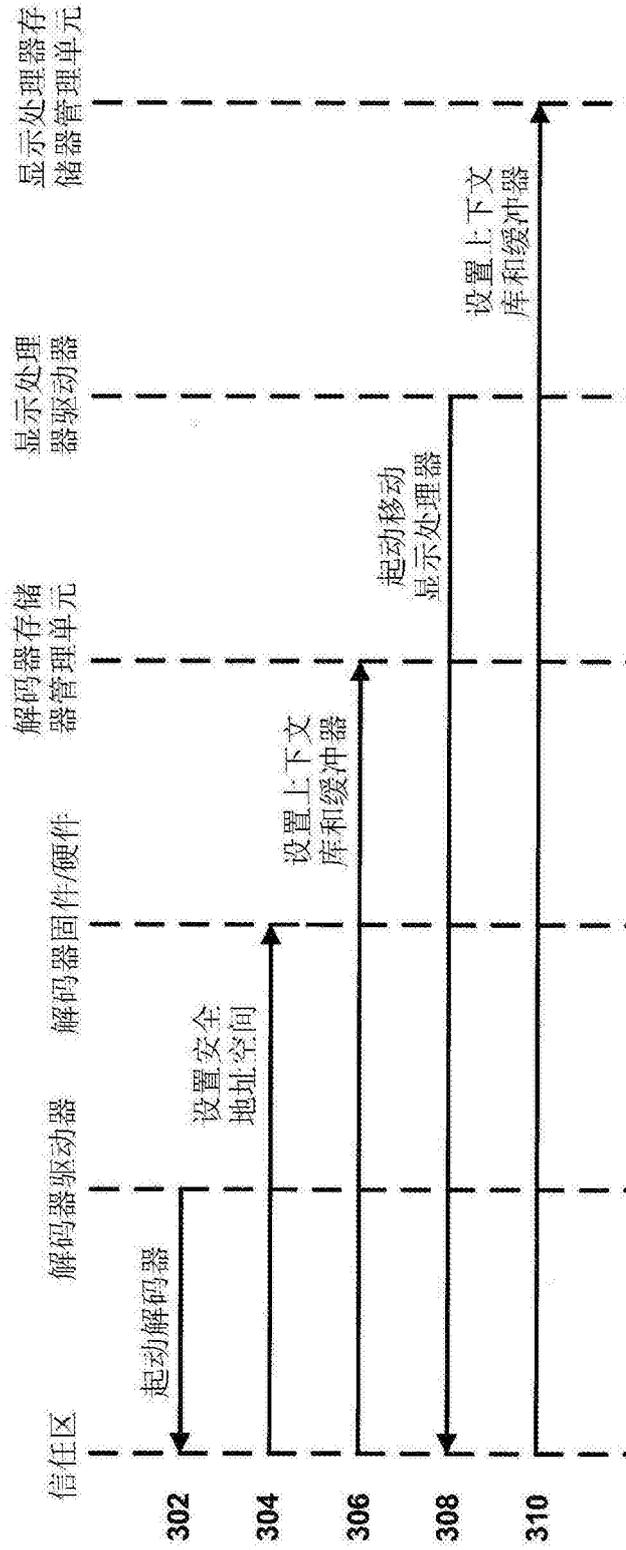


图3A

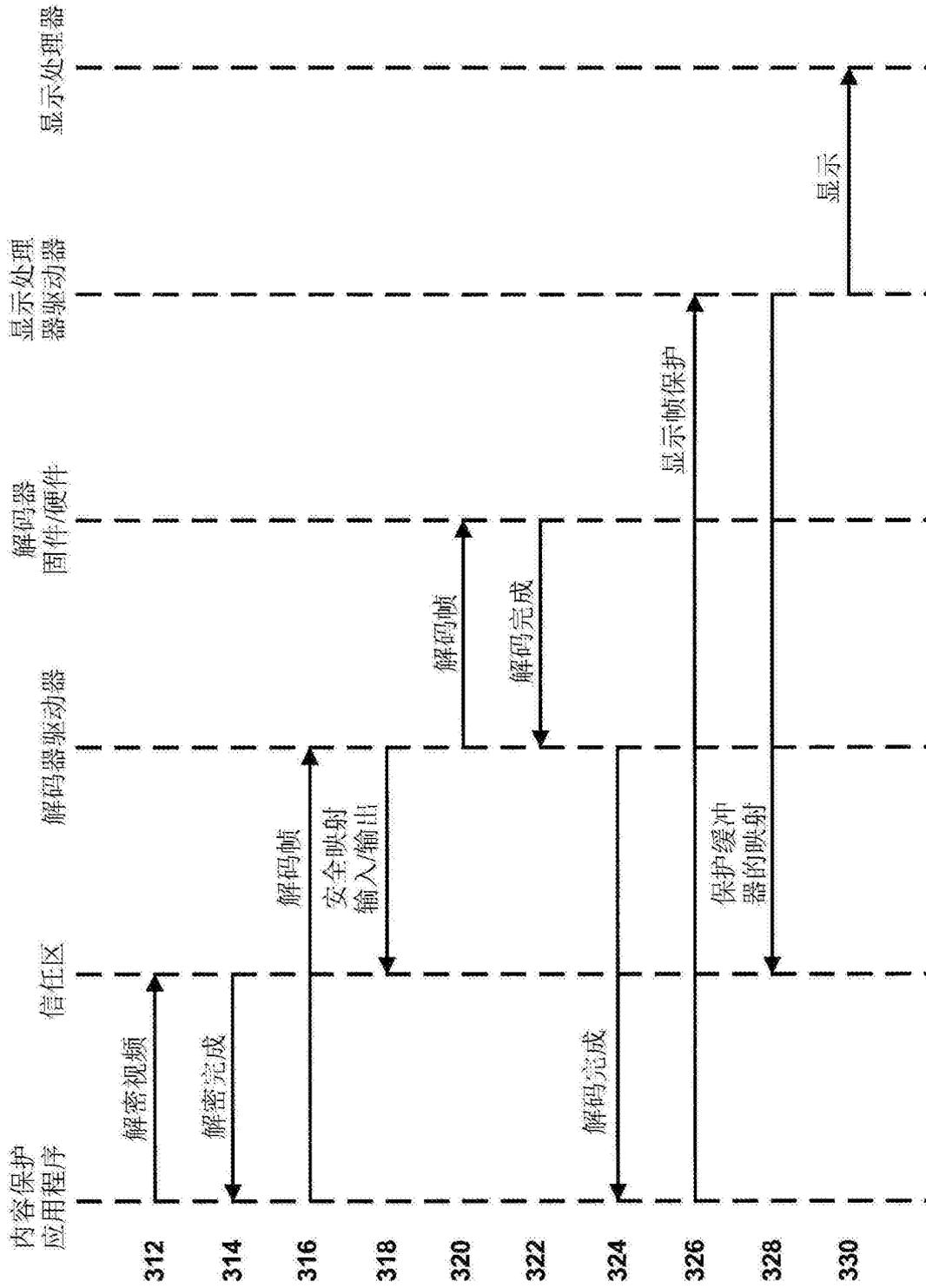


图3B

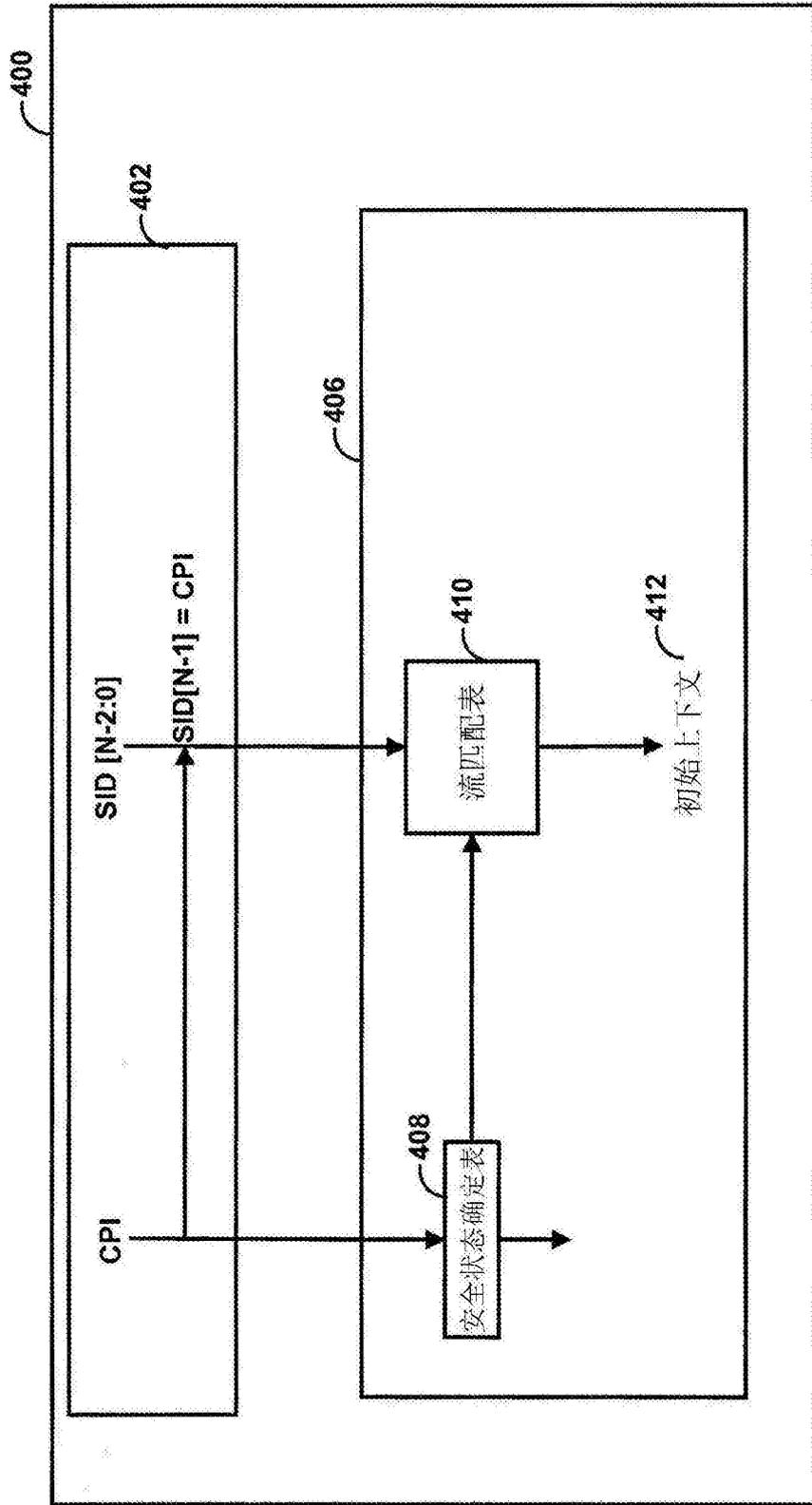


图4A

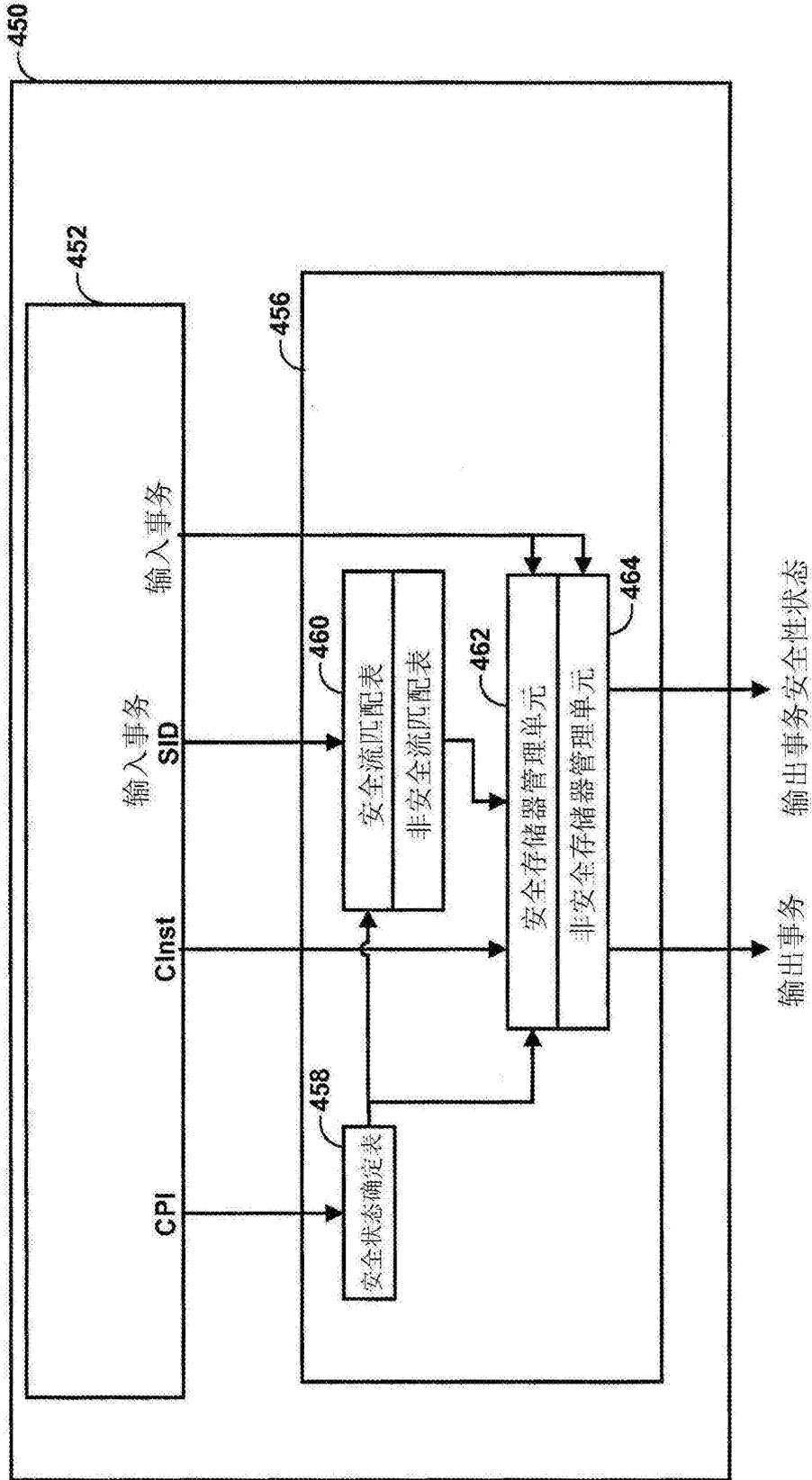


图4B

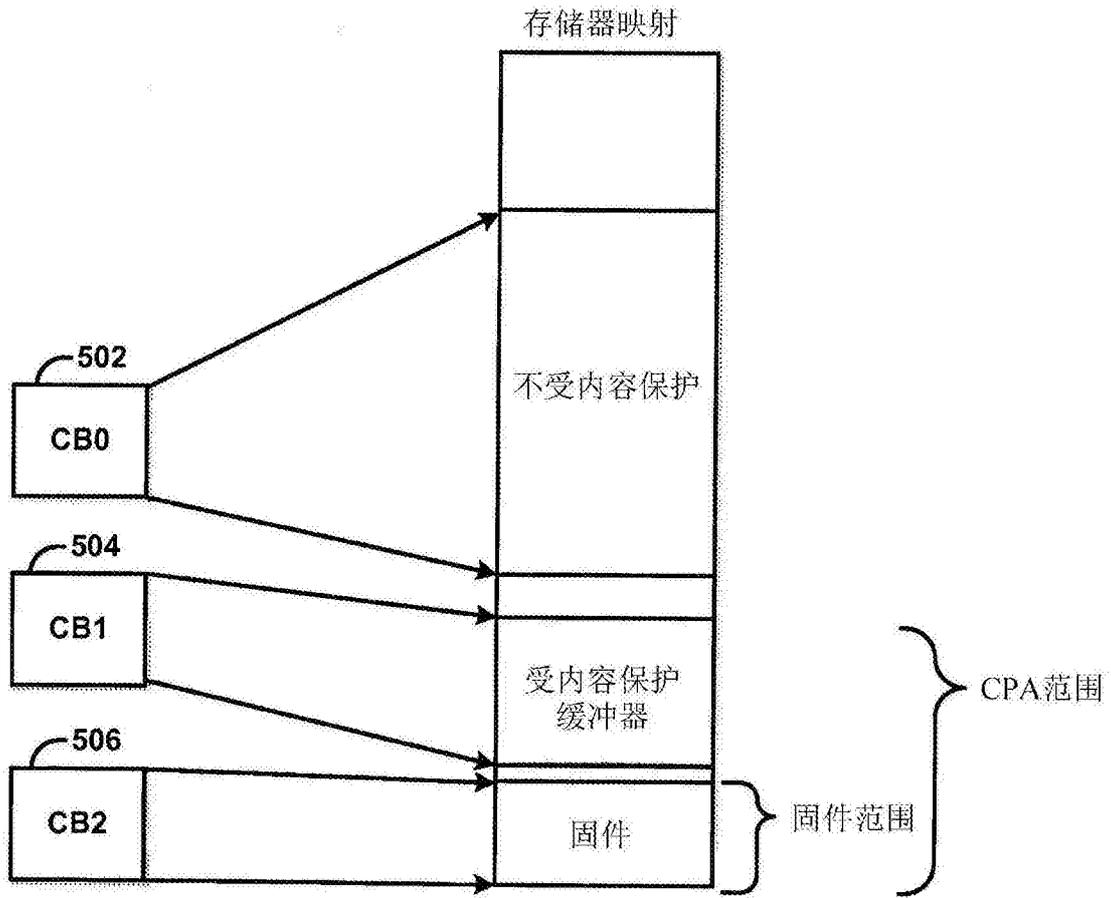


图5

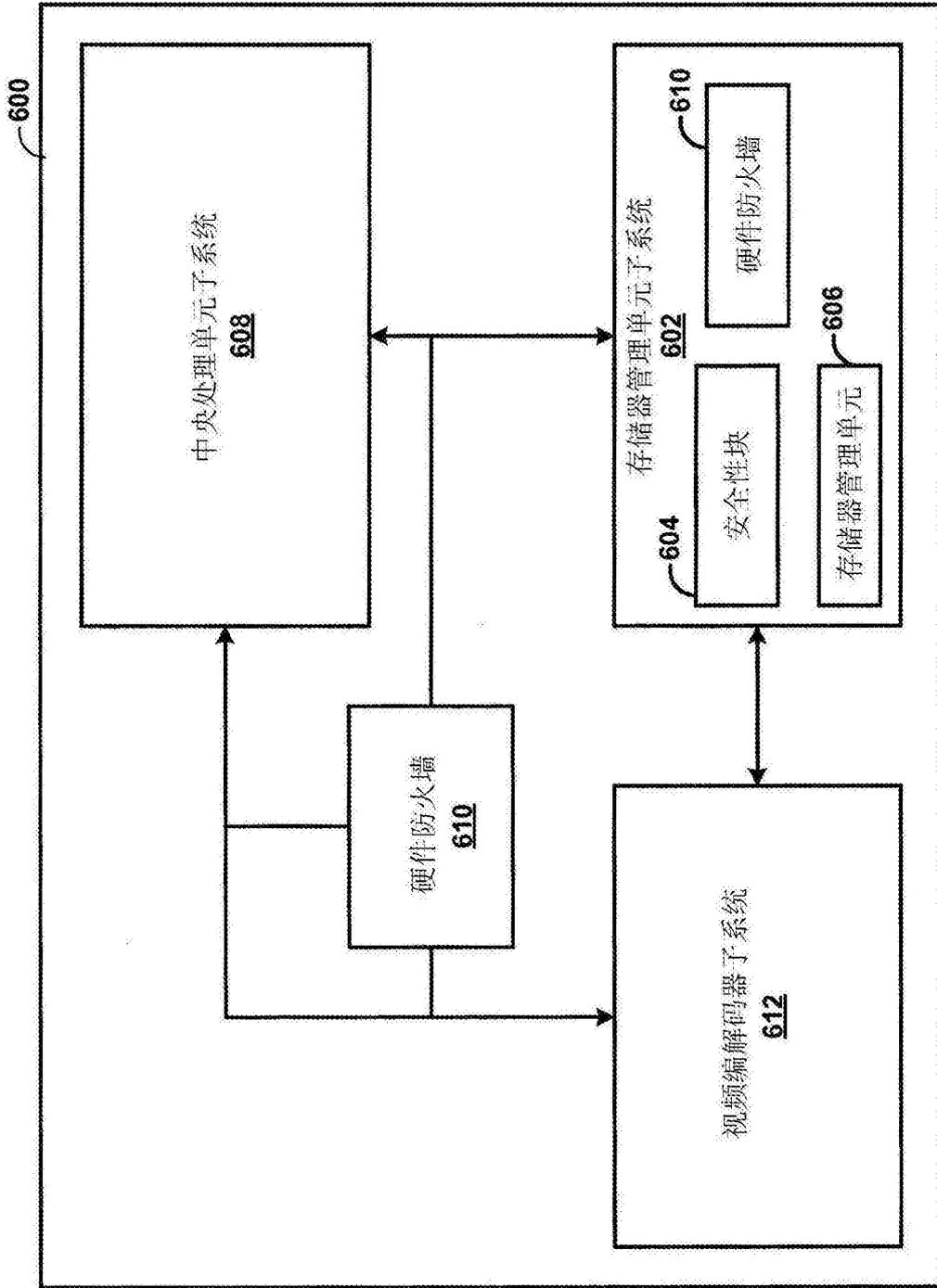


图6A

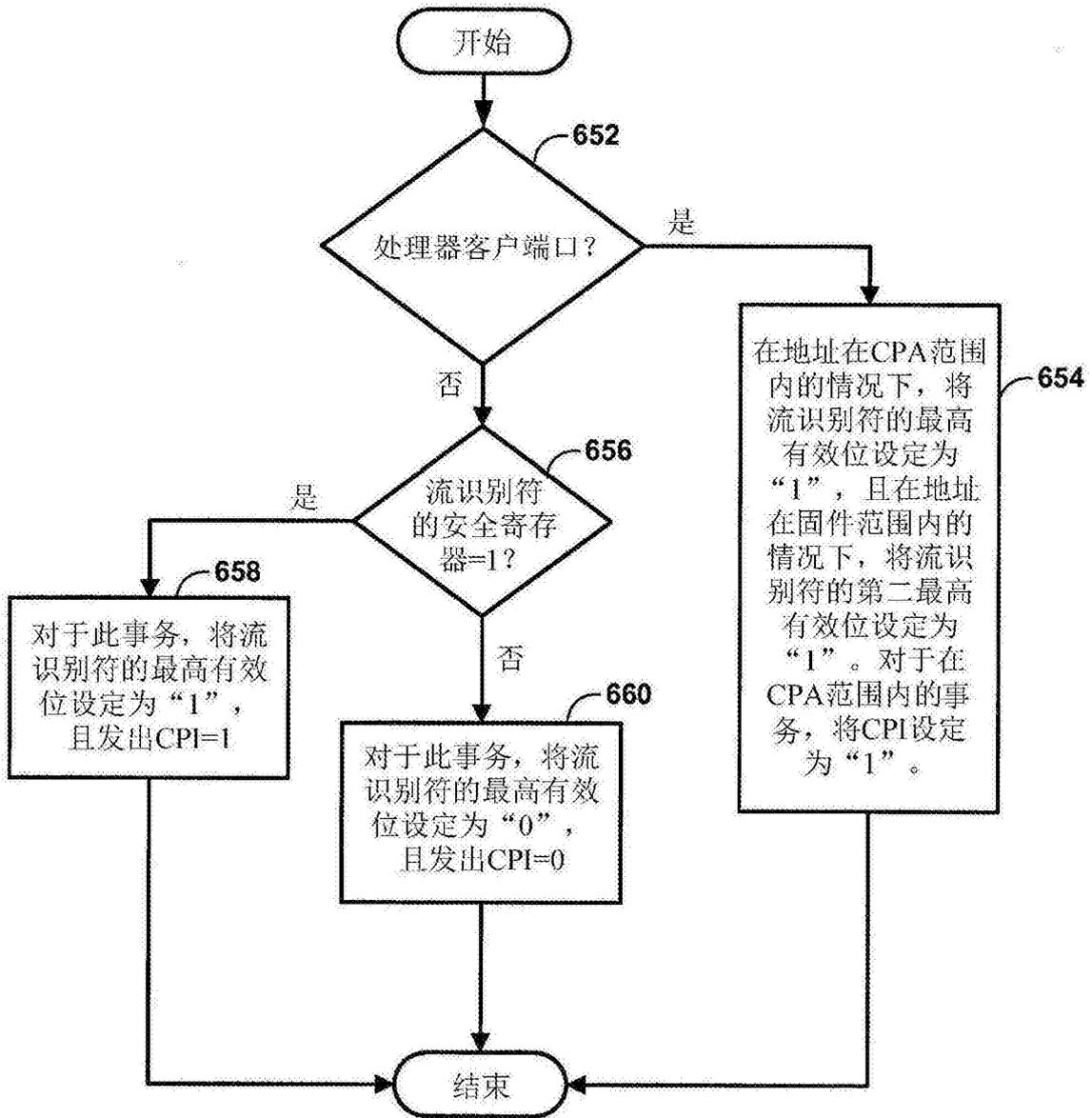


图6B

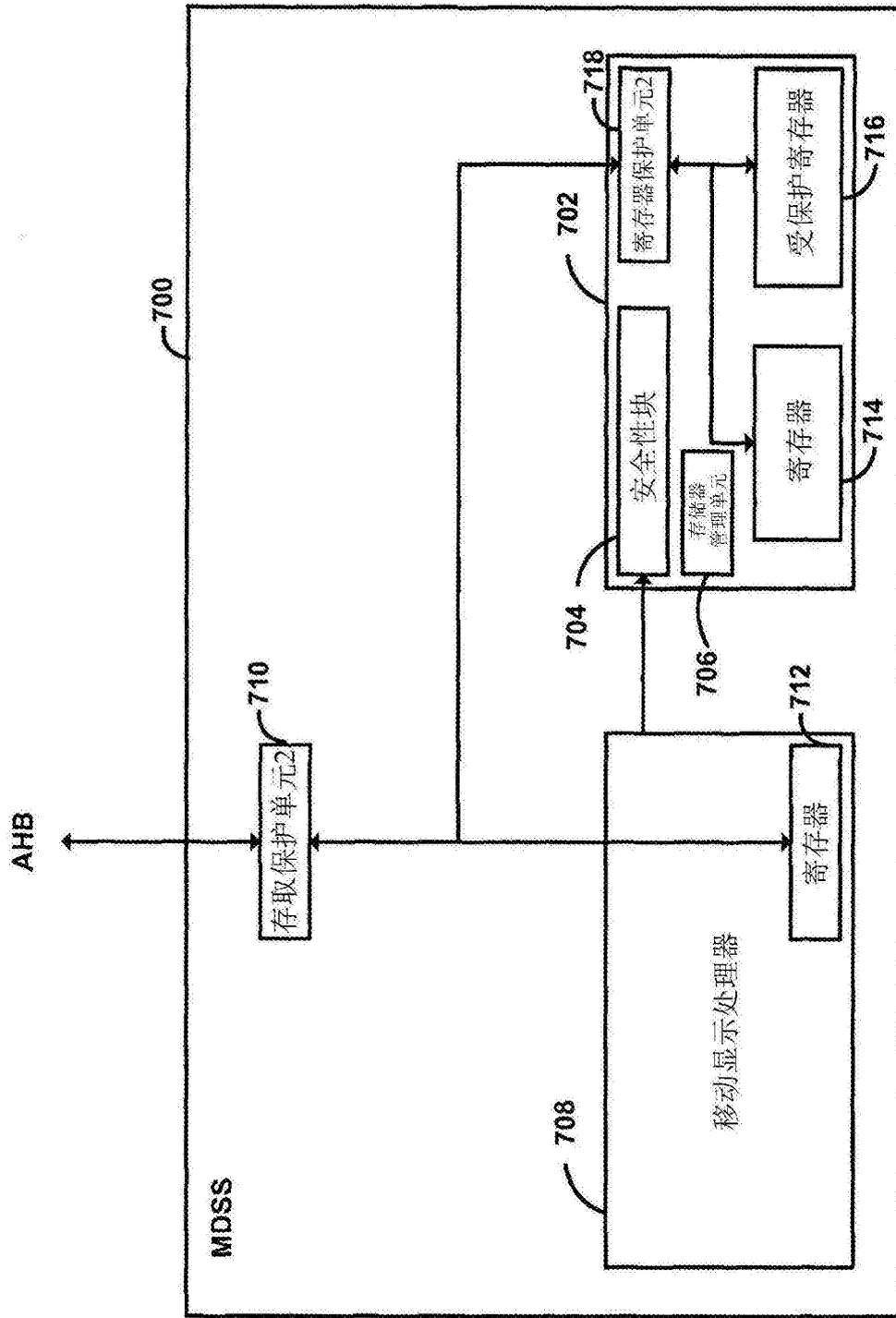


图7A

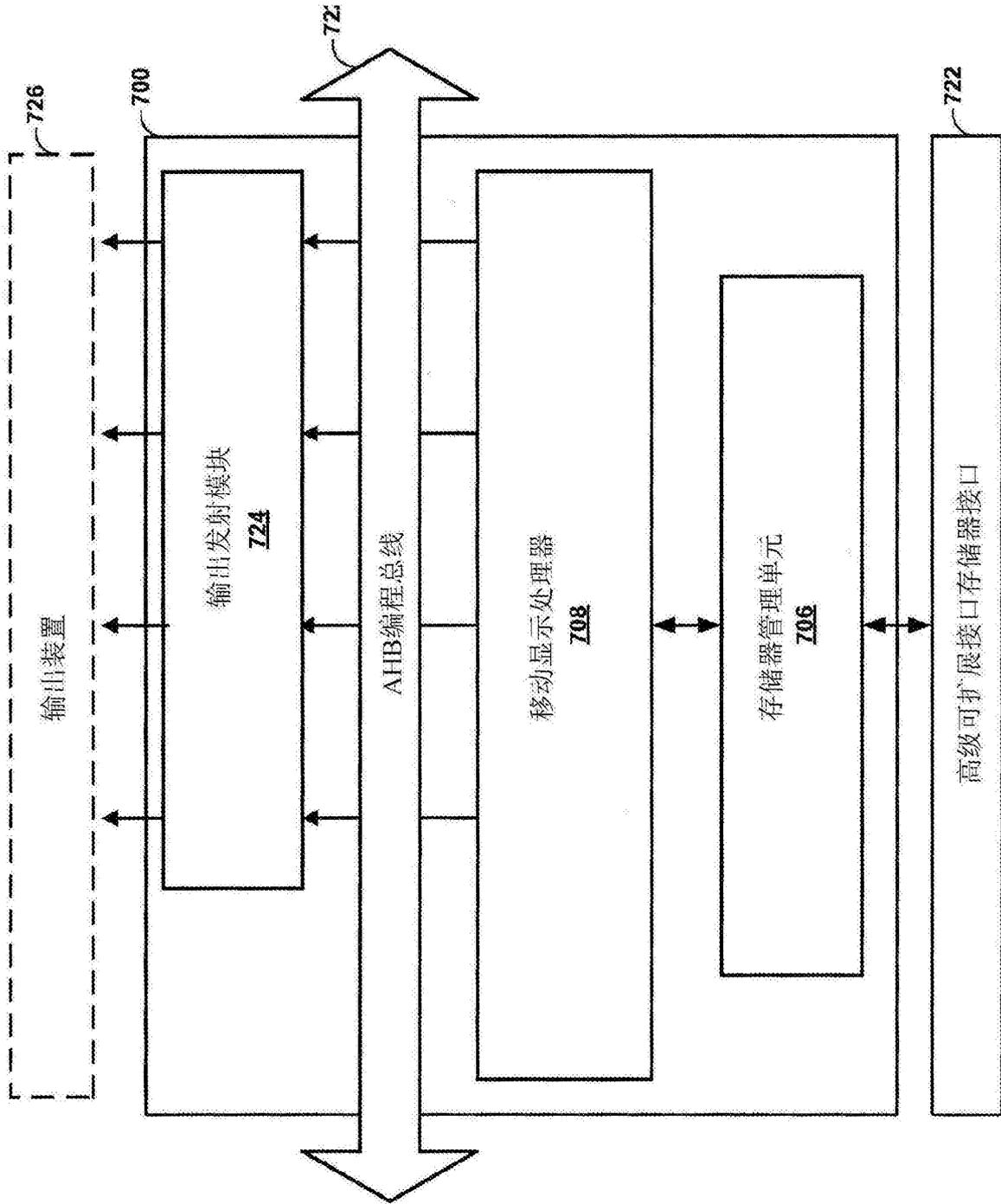


图7B

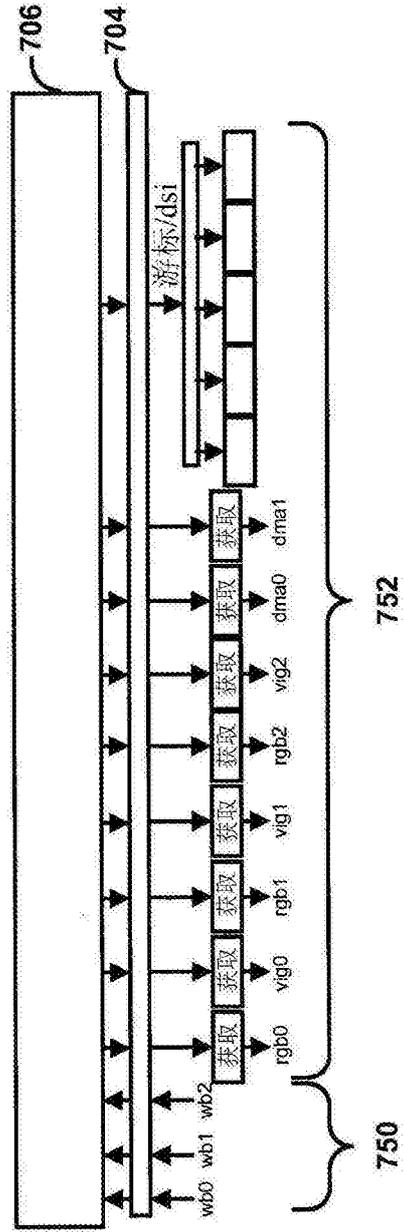


图7C

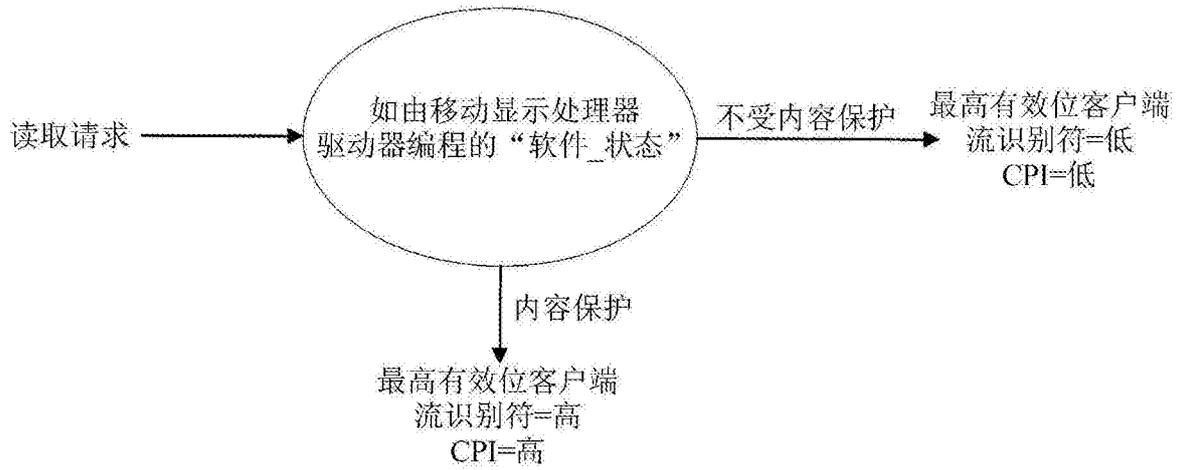


图8A

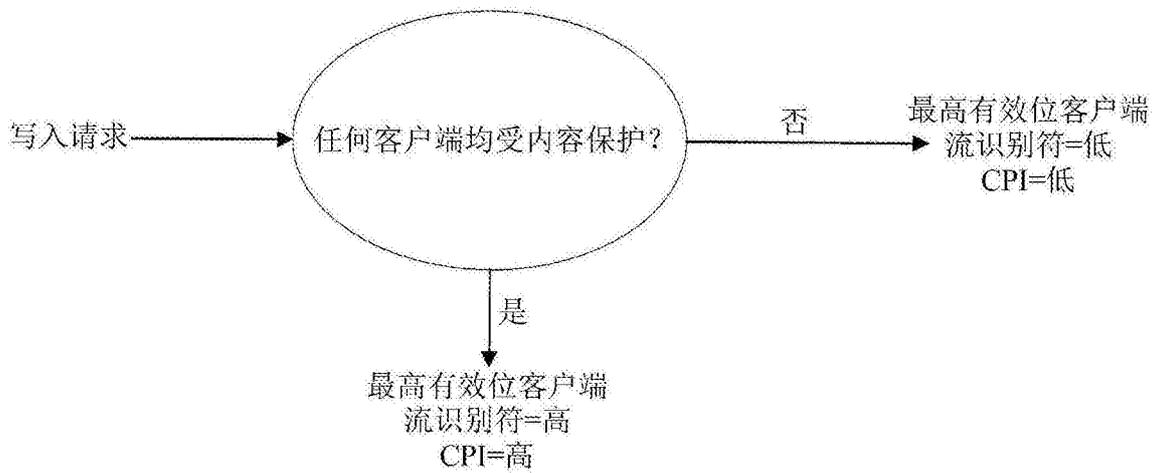


图8B

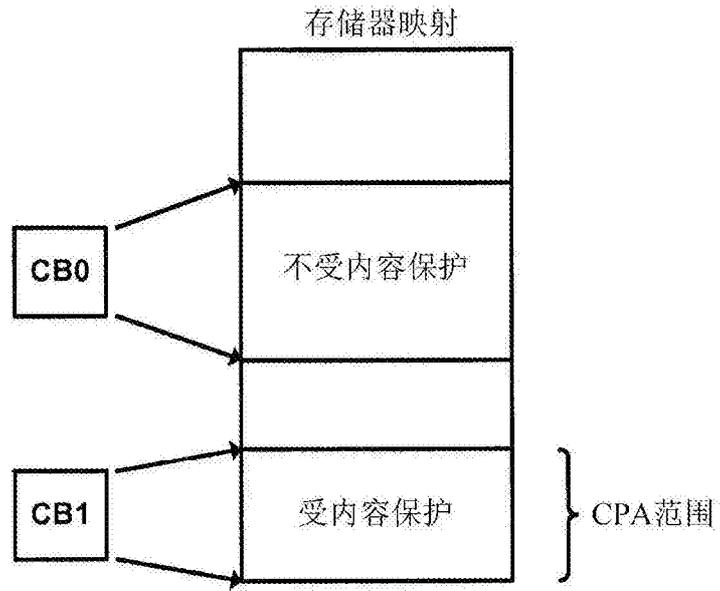


图8C

900

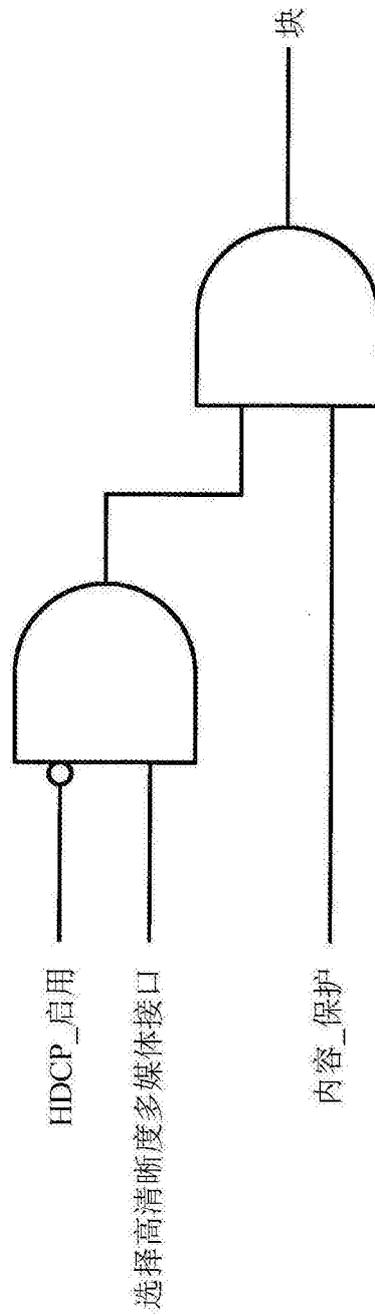


图9

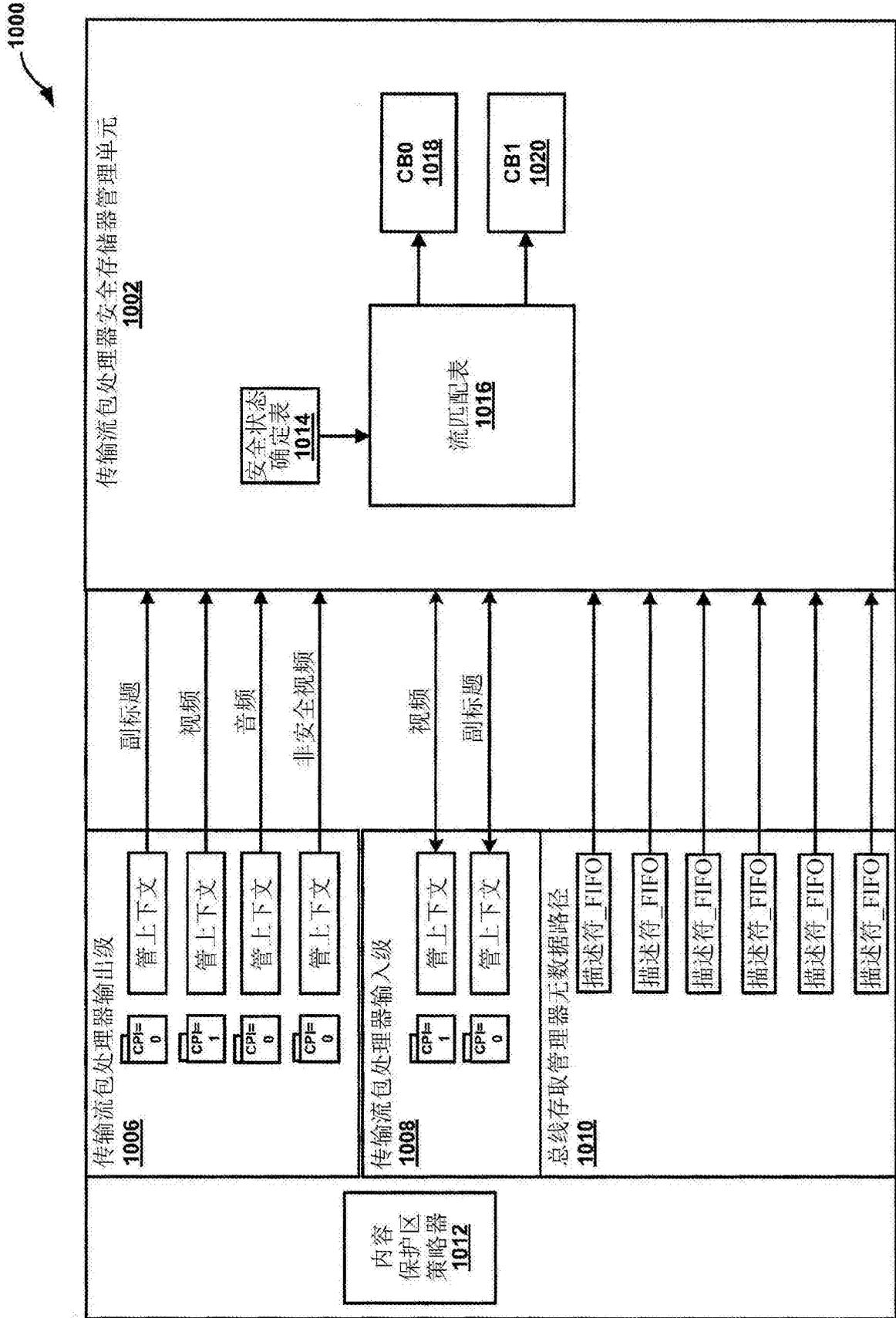


图10

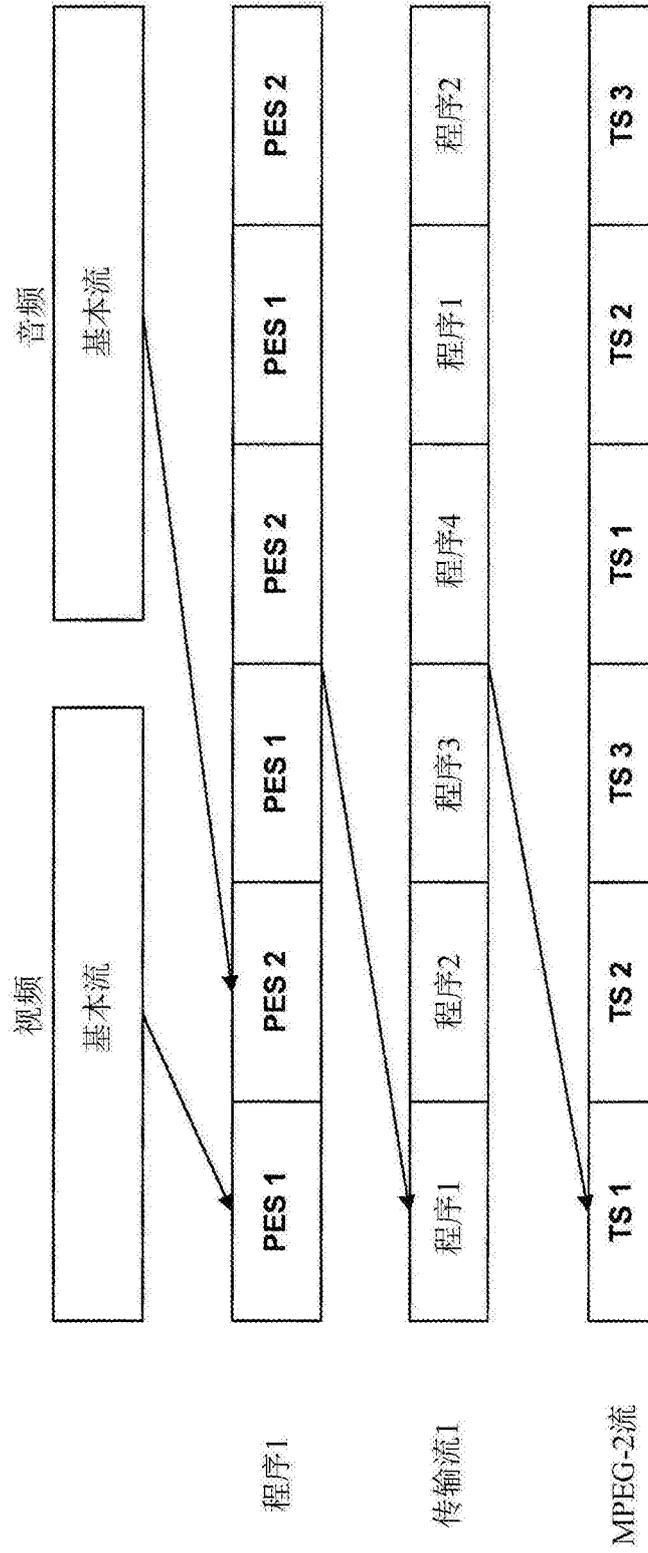


图11

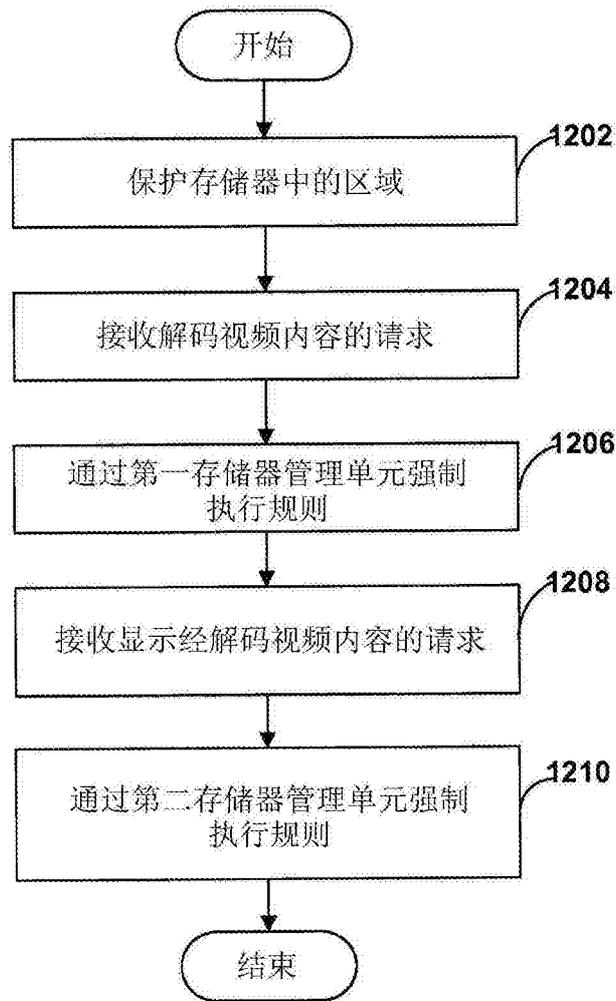


图12