РОССИЙСКАЯ ФЕДЕРАЦИЯ

(19) **RU** (11) **2004 110 622** (13) **A**

(51) МПК[7] **G 06 F 17/00**

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) ЗАЯВКА НА ИЗОБРЕТЕНИЕ

(21), (22) Заявка: **2004110622/09, 03.12.2002**

(30) Приоритет: **04.12.2001 US 60/337,617**
10.12.2001 US 60/339,143
18.04.2002 US 10/124,922

(43) Дата публикации заявки: **10.09.2005 Бюл. № 25**

(85) Дата перевода заявки PCT на национальную фазу: **07.04.2004**

(86) Заявка PCT:
US 02/38827 (03.12.2002)

(87) Публикация PCT:
WO 03/048939 (12.06.2003)

Адрес для переписки:
129010, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Г.Б. Егоровой

(71) Заявитель(и):
МАЙКРОСОФТ КОРПОРЕЙШН (US)

(72) Автор(ы):
ИНГЛЭНД Пол (US),
ПЕЙНАДО Маркус (US),
УИЛТ Николас П. (US)

(74) Патентный поверенный:
Егорова Галина Борисовна

(54) СПОСОБЫ И СИСТЕМЫ ДЛЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ОХРАНЯЕМОГО СОДЕРЖИМОГО

Формула изобретения

1. Способ криптографической защиты охраняемого содержимого в связи с достоверной графической системой вычислительного устройства, причем эта достоверная графическая система имеет видеопамять, по меньшей мере один блок графической обработки (БГО) и устройство криптографической обработки, соединенное для осуществления связи по меньшей мере с одним БГО, содержащий запрашивание графической системы программным приложением либо устройством выполнить обработку либо визуализацию охраняемого содержимого, при этом упомянутое запрашивание включает в себя передачу сеансового ключа упомянутым программным приложением либо устройством в графическую систему и передачу упомянутого охраняемого содержимого по меньшей мере в одну зашифрованную часть видеопамяти; дешифрирование содержимого упомянутой по меньшей мере из одной зашифрованной части видеопамяти упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки; выполнение по меньшей мере обработки или визуализации упомянутого дешифрированного содержимого по меньшей мере одним БГО и выведение упомянутого содержимого из по меньшей мере из одного БГО.

2. Способ по п.1, в котором, если выход при упомянутом выведении отличается от охраняемого содержимого при упомянутом запрашивании, настроенном для любой обработки, выполняемой в отношении упомянутого охраняемого содержимого упомянутым по меньшей мере одним БГО, то упомянутое программное приложение либо устройство

RU 2004110622 A

RU 2004110622 A

предупреждается об этом различии.

3. Способ по п.1, в котором упомянутая передача включает в себя передачу упомянутого охраняемого содержимого по меньшей мере к одной зашифрованной поверхности, которая перекрывает по меньшей мере одну первичную поверхность упомянутой видеопамяти.

4. Способ по п.1, в котором упомянутое дешифрирование содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти включает в себя дешифрирование геометрической части первичной поверхности, при этом пикселы иные, чем в геометрической части, не дешифрируются.

5. Способ по п.1, в котором криптографический процессор постоянно связан с графическим адаптером за счет либо (A) добавления этого криптографического процессора к существующей микросхеме, либо (B) добавления этого криптографического процессора в качестве отдельной микросхемы к графическому адаптеру, при этом физическое соединение между криптографическим процессором и остальной частью графического адаптера недоступно и не показывается.

6. Способ по п.3, в котором упомянутое дешифрирование включает в себя дешифрирование упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности механизмом дешифрирования упомянутого БГО, соединенного для осуществления связи с упомянутым устройством криптографической обработки.

7. Способ по п.3, в котором упомянутое дешифрирование включает в себя либо (A) дешифрирование упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности во время выполнения аппаратурой цифроаналогового преобразования (ЦАП) в графической системе, по мере того как содержимое выводится согласно упомянутому выведению, либо (B) дешифрирование упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности во время выполнения, непосредственно перед тем, как содержимое достигнет аппаратуры ЦАП в графической системе.

8. Способ по п.3, в котором упомянутое дешифрирование включает в себя дешифрирование упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности перед тем, как содержимое достигнет аппаратуры ЦАП в графической системе, компонентом, не имеющим обратного канала к главной компьютерной системе.

9. Способ по п.1, дополнительно содержащий повторное шифрование упомянутого содержимого упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки перед упомянутым выведением; дешифрирование упомянутого повторно зашифрованного содержимого по меньшей мере вторым устройством криптографической обработки во внешнем вычислительном устройстве.

10. Способ по п.1, в котором содержимое передается в цифровом виде к внешнему устройству, имеющему второе устройство криптографической обработки, и упомянутое дешифрирование происходит в упомянутом внешнем устройстве.

11. Способ по п.9, в котором упомянутое внешнее вычислительное устройство представляет собой либо (A) монитор, либо (B) телеприставку, либо (C) устройство визуализации цифровой обработки сигналов (ЦОС).

12. Способ по п.3, в котором упомянутая передача включает в себя передачу упомянутого охраняемого содержимого либо (A) к первому зашифрованному конфиденциальному оверлею для базовой визуализации охраняемого содержимого и (B) ко второму зашифрованному защищенному оверлею, специально спроектированному для существующих чувствительных пользовательских интерфейсов, либо (C) к первой зашифрованной области первичной поверхности для базовой визуализации охраняемого содержимого и (D) ко второй зашифрованной области первичной поверхности, специально спроектированной для существующих чувствительных пользовательских интерфейсов.

13. Способ по п.1, в котором упомянутое дешифрирование включает в себя вычисление криптографического дайджеста дешифрированных данных, а упомянутый способ дополнительно содержит передачу упомянутого криптографического дайджеста к программному приложению либо устройству, чтобы гарантировать, что отображенные

RU 2004110622 A

RU 2004110622 A

пикселы являются пикселами, переданными в связи с упомянутым запрашиванием от программного приложения либо устройства.

14. Способ по п.12, в котором упомянутый второй зашифрованный защищенный оверлей находится всегда наверху и не закрывается, и в котором содержимое второго зашифрованного защищенного оверлея проверяется упомянутым по меньшей мере одним БГО.

15. Способ по п.12, в котором упомянутое дешифрирование включает в себя либо (A) дешифрирование содержимого первого зашифрованного конфиденциального оверлея первым компонентом дешифрирования потокового шифра, либо (B) дешифрирование содержимого второго зашифрованного защищенного оверлея вторым компонентом дешифрирования потокового шифра, либо (C) дешифрирование содержимого первой зашифрованной области первичной поверхности первым компонентом дешифрирования потокового шифра, либо (D) дешифрирование содержимого второй зашифрованной области первичной поверхности вторым компонентом дешифрирования потокового шифра.

16. Способ по п.15, в котором по меньшей мере один бит каждого пиксела в первичной поверхности используется для определения членства в виртуальной защищенной поверхности для этого пиксела, причем графический адаптер выбирает подходящий ключ дешифрирования для пиксела на основании упомянутого по меньшей мере одного бита.

17. Способ по п.16, в котором, если упомянутый по меньшей мере один бит содержит нулевое значение, то виртуальная защищенная поверхность, связанная с упомянутым по меньшей мере одним битом, интерпретируется как область, не подлежащая дешифрированию.

18. Способ по п.15, дополнительно включающий, когда доступны дешифрированные пиксельные значения, выбор компонентом выбора пиксела в упомянутом по меньшей мере одном БГО пиксельного значения либо (A) второго зашифрованного защищенного оверлея, либо (B) первого зашифрованного конфиденциального оверлея, либо (3) первичной поверхности.

19. Способ по п.12, в котором упомянутое запрашивание включает в себя по меньшей мере (A) ограничивающую источник или место назначения рамку упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности, (B) целевой цветовой код упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности, (C) в случае первого зашифрованного конфиденциального оверлея, описание ключевого указателя шифрования содержимого оверлейного обратного буфера, в который должны отражаться данные, (D) в случае второго зашифрованного защищенного оверлея, описание ячейки памяти, куда записывается по меньшей мере одно из циклического избыточного кода (ЦИК), меры целостности и значения дайджеста дешифрированного содержимого оверлея, (E) ограничивающую источник или место назначения рамку по меньшей мере одной зашифрованной первичной поверхности, и (F) целевой цветовой код упомянутой по меньшей мере одной зашифрованной первичной поверхности.

20. Способ по п.19, в котором программное приложение либо устройство вычисляет по меньшей мере одно из циклического избыточного кода (ЦИК), меры целостности и значения дайджеста, если упомянутое программное приложение либо устройство имеет отношение к целостности содержимого.

21. Способ по п.1, в котором по меньшей мере один командный буфер, посланный в блок видео декодера по меньшей мере одного БГО, присущего упомянутому запрашиванию, зашифровывается упомянутым программным приложением либо устройством и дешифрируется упомянутым блоком видео декодера при осуществлении связи с упомянутым блоком криптографической обработки.

22. Способ по п.21, содержащий далее обнаружение несанкционированного доступа к упомянутому по меньшей мере одному командному буферу либо (A) с помощью двух проходов перед использованием по меньшей мере одного командного буфера, либо (B) после того, как командный буфер использован.

23. По меньшей мере одно из операционной системы, машиночитаемого носителя данных с сохраненными на нем множеством исполняемых компьютером команд,

RU 2004110622 A

RU 2004110622 A

сопроцессорного устройства, вычислительного устройства и модулированного сигнала данных, несущего исполняемые компьютером команды, для выполнения способа по п.1.

24. Способ криптографической защиты охраняемого содержимого в связи с достоверной графической системой вычислительного устройства, причем эта достоверная графическая система имеет видеопамять, по меньшей мере один блок графической обработки (БГО) и устройство криптографической обработки, соединенное для осуществления связи по меньшей мере с одним БГО, содержащий запрашивание графической системы программным приложением либо устройством выполнить обработку либо визуализацию охраняемого содержимого, при этом упомянутое запрашивание включает в себя передачу сеансового ключа упомянутым программным приложением либо устройством в графическую систему для проверки устройством криптографической обработки и передачу упомянутого охраняемого содержимого по меньшей мере в одну зашифрованную часть видеопамяти; дешифрирование содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти механизмом дешифрирования входного блока в упомянутом по меньшей мере одном БГО, при этом упомянутый механизм дешифрирования осуществляет связь с упомянутым устройством криптографической обработки; выполнение по меньшей мере обработки или визуализации упомянутого дешифрированного содержимого по меньшей мере одним БГО; шифрование упомянутого содержимого механизмом шифрования-дешифрирования выходного блока в по меньшей мере одном БГО и выведение упомянутого зашифрованного содержимого по меньшей мере из одного БГО.

25. Способ по п.24, в котором упомянутый входной блок является блоком текстурного преобразования, а упомянутый выходной блок является блоком альфа-канала, и при этом упомянутая по меньшей мере одна зашифрованная часть упомянутой видеопамяти является зашифрованной текстурной поверхностью.

26. Способ по п.24, в котором упомянутое охраняемое содержимое является либо текстурными данными, либо открытым текстом, либо видео макроблоками.

27. Способ по п.24, в котором упомянутые шифрование и дешифрирование включают в себя, соответственно, шифрование и дешифрирование с помощью блоковых шифров.

28. Способ по п.25, в котором механизм дешифрирования блока текстурного преобразования дешифрирует заполнение строки кэш-памяти, и в котором механизм шифрования-дешифрирования блока альфа-канала осуществляет шифрование перед записью.

29. Способ по п.25, дополнительно включающий дешифрирование механизмом шифрования-дешифрирования блока альфа-канала при считывании строки кэш-памяти из цветового буфера в видеопамяти.

30. Способ по п.24, дополнительно включающий отражение упомянутого зашифрованного выходного содержимого из зашифрованной задней первичной поверхности в зашифрованную переднюю первичную поверхность упомянутой видеопамяти; второе дешифрирование упомянутого зашифрованного выходного содержимого вторым механизмом дешифрирования упомянутого по меньшей мере одного БГО при осуществлении связи с упомянутым устройством криптографической обработки и второе выведение упомянутого выходного содержимого.

31. Способ по п.24, в котором упомянутое выведение включает в себя выведение зашифрованного содержимого в цепочку, отражающую конфиденциальный оверлей, а способ дополнительно включает отражение упомянутого зашифрованного выходного содержимого из зашифрованной задней конфиденциальной поверхности в зашифрованную переднюю конфиденциальную поверхность, при этом упомянутое шифрование упомянутым механизмом шифрования-дешифрирования включает в себя шифрование, использующее шифрование потоковым шифром; второе дешифрирование упомянутого зашифрованного выходного содержимого механизмом дешифрирования потокового шифра в упомянутом по меньшей мере одном БГО при осуществлении связи с упомянутым устройством криптографической обработки.

32. Способ по п.31, дополнительно содержащий перед упомянутым шифрованием,

RU 2004110622 A

RU 2004110622 A

кодирование местоположения в содержимом; после упомянутого второго дешифрирования, декодирование этого местоположения в содержимом, при этом упомянутое местоположение является недоступным извне, предохраняя целостность преобразования открытого текста в зашифрованный текст.

33. Способ по п.24, в котором, если выход при упомянутом выведении отличается от охраняемого содержимого при упомянутом запрашивании, настроенном для любой обработки, выполняемой в отношении упомянутого охраняемого содержимого упомянутым по меньшей мере одним БГО, то упомянутое программное приложение либо устройство предупреждается об этом различии.

34. Способ по п.24, дополнительно включающий повторное шифрование упомянутого содержимого упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки перед упомянутым выведением; дешифрирование упомянутого повторно зашифрованного содержимого по меньшей мере вторым устройством криптографической обработки во внешнем вычислительном устройстве.

35. Способ по п.34, в котором упомянутое внешнее вычислительное устройство представляет собой либо (A) монитор, либо (B) телеприставку, либо (C) устройство визуализации цифровой обработки сигналов (ЦОС).

36. Способ по п.24, в котором зашифрованные текстуры и зашифрованные внеэкранные поверхности, доставленные упомянутым программным приложением либо устройством, кодируются блоковыми шифрами, а упомянутое программное приложение либо устройство смешивает эти блоковые шифры с заранее определенным форматом смешивания, который преобразует местоположение (x,y) в содержимом в сдвиг по меньшей мере для YUV, RGB, YUY2 и упакованного планарного форматов.

37. Способ по п.24, в котором по меньшей мере один командный буфер, посланный в блок видео декодера по меньшей мере одного БГО соответственно упомянутому запрашиванию, зашифровывается упомянутым программным приложением либо устройством и дешифрируется упомянутым блоком видео декодера при осуществлении связи с упомянутым блоком криптографической обработки.

38. Способ по п.24, дополнительно включающий обнаружение несанкционированного доступа к упомянутому по меньшей мере одному командному буферу либо (A) с помощью двух проходов перед использованием по меньшей мере одного командного буфера, либо (B) после того, как командный буфер использован.

39. По меньшей мере одно из операционной системы, машиночитаемого носителя данных с сохраненными на нем множеством исполняемых компьютером команд, сопроцессорное устройство, вычислительное устройство и модулированный сигнал данных, несущий исполняемые компьютером команды для выполнения способа по п.24.

40. По меньшей мере один машиночитаемый носитель данных, содержащий исполняемые компьютером модули, в том числе исполняемые компьютером команды для криптографической защиты охраняемого содержимого в связи с достоверной графической системой вычислительного устройства, причем эта достоверная графическая система имеет видеопамять, по меньшей мере один блок графической обработки (БГО) и устройство криптографической обработки, соединенное для осуществления связи с упомянутым по меньшей мере одним БГО, при этом исполняемые компьютером модули содержат средство для запрашивания графической системы программным приложением либо устройством выполнить обработку, либо визуализацию охраняемого содержимого, при этом упомянутое средство для запрашивания включает в себя средство для передачи сеансового ключа упомянутым программным приложением, либо устройством в графическую систему и средство для передачи упомянутого охраняемого содержимого по меньшей мере в одну зашифрованную часть видеопамяти; средство для дешифрирования содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти упомянутым по меньшей мере одним БГО при осуществлении связи с упомянутым устройством криптографической обработки; средство для выполнения по меньшей мере обработки или визуализации упомянутого дешифрированного содержимого по меньшей

RU 2004110622 A
RU 2004110622 A

мере одним БГО; средство для выведения упомянутого содержимого по меньшей мере из одного БГО.

41. По меньшей мере один машиночитаемый носитель данных по п.40, в котором, если выход упомянутого средства для выведения отличается от охраняемого содержимого в упомянутом средстве для запрашивания, настроенном для любой обработки, выполняемой на упомянутом охраняемом содержимом упомянутым по меньшей мере одним БГО, то упомянутое программное приложение либо устройство предупреждается об этом различии.

42. По меньшей мере один машиночитаемый носитель данных по п.40, в котором упомянутое средство для передачи включает в себя средство для передачи упомянутого охраняемого содержимого по меньшей мере к одной зашифрованной поверхности, которая перекрывает по меньшей мере одну первичную поверхность упомянутой видеопамяти.

43. По меньшей мере один машиночитаемый носитель данных по п.40, в котором упомянутое средство для дешифрирования содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти включает в себя средство для дешифрирования геометрической части первичной поверхности, при этом пикселы иные, чем в геометрической части, не дешифрируются.

44. По меньшей мере один машиночитаемый носитель данных по п.40, в котором криптографический процессор постоянно связан с графическим адаптером либо (A) добавлением этого криптографического процессора к существующей микросхеме, либо (B) добавлением этого криптографического процессора в качестве отдельной микросхемы к графическому адаптеру, благодаря чему физическое соединение между криптографическим процессором и остальной частью графического адаптера недоступно и не показывается.

45. По меньшей мере один машиночитаемый носитель данных по п.42, в котором упомянутое средство для дешифрирования включает в себя средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности механизмом дешифрирования упомянутого БГО, соединенного для осуществления связи с упомянутым устройством криптографической обработки.

46. По меньшей мере один машиночитаемый носитель данных по п.42, в котором упомянутое средство для дешифрирования включает в себя либо (A) средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности во время выполнения аппаратурой цифроаналогового преобразования (ЦАП) в графической системе, по мере того как содержимое выводится согласно упомянутому выведению, либо (B) средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности во время выполнения непосредственно перед тем, как содержимое достигнет аппаратуры ЦАП в графической системе.

47. По меньшей мере один машиночитаемый носитель данных по п.42, в котором упомянутое средство для дешифрирования включает в себя средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности перед тем, как содержимое достигнет аппаратуры ЦАП в графической системе, компонентом, не имеющим обратного канала к главной компьютерной системе.

48. По меньшей мере один машиночитаемый носитель данных по п.40, дополнительно содержащий средство для повторного шифрования упомянутого содержимого упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки перед упомянутым выведением упомянутым средством для выведения; средство для дешифрирования упомянутого повторно зашифрованного содержимого по меньшей мере вторым устройством криптографической обработки во внешнем вычислительном устройстве.

49. По меньшей мере один машиночитаемый носитель данных по п.40, в котором содержимое передается в цифровом виде к внешнему устройству, имеющему второе устройство криптографической обработки, а упомянутое дешифрирование упомянутого средства для дешифрирования осуществляется в упомянутом внешнем устройстве.

50. По меньшей мере один машиночитаемый носитель данных по п.48, в котором упомянутое внешнее вычислительное устройство представляет собой либо (A) монитор,

RU 2004110622 A

RU 2004110622 A

либо (B) телеприставку, либо (C) устройство визуализации цифровой обработки сигналов (ЦОС).

51. По меньшей мере один машиночитаемый носитель данных по п.42, в котором упомянутое средство для передачи включает в себя средство для передачи упомянутого охраняемого содержимого либо (A) к первому зашифрованному конфиденциальному оверлею для базовой визуализации охраняемого содержимого и (B) ко второму зашифрованному защищенному оверлею, специально спроектированному для существующих чувствительных пользовательских интерфейсов, либо (C) к первой зашифрованной области первичной поверхности для базовой визуализации охраняемого содержимого и (D) ко второй зашифрованной области первичной поверхности, специально спроектированной для существующих чувствительных пользовательских интерфейсов.

52. По меньшей мере один машиночитаемый носитель данных по п.40, в котором упомянутое средство для дешифрирования включает в себя средство для вычисления криптографического дайджеста дешифрированных данных, а упомянутые исполняемые компьютером модули дополнительно содержат средство для передачи упомянутого криптографического дайджеста к программному приложению либо устройству, чтобы гарантировать, что отображенные пикселы являются пикселами, переданными в связи с упомянутым запрашиванием от программного приложения либо устройства через упомянутое средство для запрашивания.

53. По меньшей мере один машиночитаемый носитель данных по п.51, в котором упомянутый второй зашифрованный защищенный оверлей находится всегда наверху и не закрывается, и содержимое второго зашифрованного защищенного оверлея проверяется упомянутым по меньшей мере одним БГО.

54. По меньшей мере один машиночитаемый носитель данных по п.51, в котором упомянутое средство для дешифрирования включает в себя либо (A) средство для дешифрирования содержимого первого зашифрованного конфиденциального оверлея первым компонентом дешифрирования потокового шифра, либо (B) средство для дешифрирования содержимого второго зашифрованного защищенного оверлея вторым компонентом дешифрирования потокового шифра, либо (C) средство для дешифрирования содержимого первой зашифрованной области первичной поверхности первым компонентом дешифрирования потокового шифра, либо (D) средство для дешифрирования содержимого второй зашифрованной области первичной поверхности вторым компонентом дешифрирования потокового шифра.

55. По меньшей мере один машиночитаемый носитель данных по п.54, в котором по меньшей мере один бит каждого пиксела в первичной поверхности используется для определения членства в виртуальной защищенной поверхности для этого пиксела, причем графический адаптер выбирает подходящий ключ дешифрирования для пиксела на основании упомянутого по меньшей мере одного бита.

56. По меньшей мере один машиночитаемый носитель данных по п.55, в котором, если упомянутый по меньшей мере один бит содержит нулевое значение, то виртуальная защищенная поверхность, связанная с упомянутым по меньшей мере одним битом, интерпретируется как область, не подлежащая дешифрированию.

57. По меньшей мере один машиночитаемый носитель данных по п.54, дополнительно содержащий средство для выбора, когда доступны дешифрированные пиксельные значения, компонентом выбора пиксела в упомянутом по меньшей мере одном БГО пиксельного значения либо (A) второго зашифрованного защищенного оверлея, либо (B) первого зашифрованного конфиденциального оверлея, либо (3) первичной поверхности.

58. По меньшей мере один машиночитаемый носитель данных по п.51, в котором упомянутое запрашивание упомянутого средства для запрашивания включает в себя по меньшей мере (A) ограничивающую источник или место назначения рамку упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности, (B) целевой цветовой код упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности, (C) в случае первого зашифрованного конфиденциального оверлея, описание ключевого указателя шифрования содержимого оверлейного обратного буфера, в который

RU 2004110622 A

RU 2004110622 A

должны отражаться данные, (D) в случае второго зашифрованного защищенного оверлея, описание ячейки памяти, куда записывается по меньшей мере одно из циклического избыточного кода (ЦИК), меры целостности и значения дайджеста дешифрированного содержимого оверлея, (E) ограничивающую источник или место назначения рамку по меньшей мере одной зашифрованной первичной поверхности, и (F) целевой цветовой код упомянутой по меньшей мере одной зашифрованной первичной поверхности.

59. По меньшей мере один машиночитаемый носитель данных по п.58, в котором программное приложение либо устройство вычисляет по меньшей одно из циклического избыточного кода (ЦИК), меры целостности и значения дайджеста, если упомянутое программное приложение либо устройство имеет отношение к целостности содержимого.

60. По меньшей мере один машиночитаемый носитель данных по п.40, в котором по меньшей мере один командный буфер, переданный в блок видео декодера по меньшей мере одного БГО соответственно упомянутому запрашиванию, зашифровывается упомянутым программным приложением либо устройством и дешифрируется упомянутым блоком видео декодера при осуществлении связи с упомянутым блоком криптографической обработки.

61. По меньшей мере один машиночитаемый носитель данных по п.60, дополнительно содержащий средство для обнаружения несанкционированного доступа к упомянутому по меньшей мере одному командному буферу либо (A) с помощью двух проходов перед использованием по меньшей мере одного командного буфера, либо (B) после того, как командный буфер использован.

62. По меньшей мере одно из операционной системы, машиночитаемого носителя данных с сохраненными на нем множеством исполняемых компьютером команд, сопроцессорное устройство, вычислительное устройство и модулированный сигнал данных, несущий исполняемые компьютером модули по меньшей мере одного машиночитаемого носителя данных по п.40.

63. По меньшей мере один машиночитаемый носитель данных, содержащий исполняемые компьютером модули, в том числе исполняемые компьютером команды для криптографической защиты охраняемого содержимого в связи с достоверной графической системой вычислительного устройства, причем эта достоверная графическая система имеет видеопамять, по меньшей мере один блок графической обработки (БГО) и устройство криптографической обработки, соединенное для осуществления связи с упомянутым по меньшей мере одним БГО, при этом исполняемые компьютером модули содержат средство для запрашивания графической системы программным приложением либо устройством выполнить обработку либо визуализацию охраняемого содержимого, при этом упомянутое средство для запрашивания включает в себя средство для передачи сеансового ключа упомянутым программным приложением либо устройством в графическую систему для проверки устройством криптографической обработки и для передачи упомянутого охраняемого содержимого по меньшей мере в одну зашифрованную часть видеопамяти; средство для дешифрирования содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти механизмом дешифрирования входного блока в упомянутом по меньшей мере одним БГО, при этом упомянутый механизм дешифрирования осуществляет связь с упомянутым устройством криптографической обработки; средство для выполнения по меньшей мере обработки или визуализации упомянутого дешифрированного содержимого по меньшей мере одним БГО; средство для шифрования упомянутого содержимого механизмом шифрования-дешифрирования выходного блока в по меньшей мере одном БГО; средство для выведения упомянутого зашифрованного содержимого по меньшей мере из одного БГО.

64. По меньшей мере один машиночитаемый носитель данных по п.63, в котором упомянутый входной блок является блоком отображения текстуры, а упомянутый выходной блок является блоком альфа-канала, и при этом упомянутая по меньшей мере одна зашифрованная часть упомянутой видеопамяти является зашифрованной текстурной поверхностью.

65. По меньшей мере один машиночитаемый носитель данных по п.63, в котором

RU 2004110622 A
RU 2004110622 A

упомянутое охраняемое содержимое является либо текстурными данными, либо открытым текстом, либо видео макроблоками.

66. По меньшей мере один машиночитаемый носитель данных по п.63, в котором упомянутые средство для шифрования и средство для дешифрирования включают в себя, соответственно, средство для шифрования и средство для дешифрирования с помощью блоковых шифров.

67. По меньшей мере один машиночитаемый носитель данных по п.63, в котором упомянутый механизм дешифрирования блока отображения текстуры дешифрирует заполнение строки кэш-памяти, и механизм шифрования-дешифрирования блока альфа-канала осуществляет шифрование перед записью.

68. По меньшей мере один машиночитаемый носитель данных по п.64, дополнительно содержит средство для дешифрирования механизмом шифрования-дешифрирования блока альфа-канала при считывании строки кэш-памяти из цветового буфера в видеопамяти.

69. По меньшей мере один машиночитаемый носитель данных по п.63, дополнительно содержащий средство для отражения упомянутого зашифрованного выходного содержимого из зашифрованной задней первичной поверхности в зашифрованную переднюю первичную поверхность упомянутой видеопамяти; второе средство для дешифрирования упомянутого зашифрованного выходного содержимого вторым механизмом дешифрирования упомянутого по меньшей мере одного БГО при осуществлении связи с упомянутым устройством криптографической обработки; второе средство для выведения упомянутого выходного содержимого.

70. По меньшей мере один машиночитаемый носитель данных по п.63, в котором упомянутое средство для выведения включает в себя средство для выведения зашифрованного содержимого в цепочку, отражающую конфиденциальный оверлей, а исполняемые компьютером модули дополнительно включают в себя средство для отражения упомянутого зашифрованного выходного содержимого из зашифрованной задней конфиденциальной поверхности в зашифрованную переднюю конфиденциальную поверхность, в соответствии с чем упомянутое шифрование упомянутым механизмом шифрования-дешифрирования включает в себя средство для шифрования, использующее шифрование потоковым шифром; второе средство для дешифрирования упомянутого зашифрованного выходного содержимого механизмом дешифрирования потокового шифра в упомянутом по меньшей мере одном БГО при осуществлении связи с упомянутым устройством криптографической обработки.

71. По меньшей мере один машиночитаемый носитель данных по п.70, содержащий далее средство для кодирования местоположения в содержимом перед упомянутым шифрованием упомянутым средством для шифрования; средство для декодирования этого местоположения в содержимом после упомянутого второго дешифрирования упомянутым вторым средством для дешифрирования, при этом упомянутое местоположение является недоступным извне сохраняя целостность преобразования открытого текста в зашифрованный текст.

72. По меньшей мере один машиночитаемый носитель данных по п.63, в котором, если выход упомянутого средства для выведения отличается от охраняемого содержимого упомянутого средства для запрашивания, настроенного для любой обработки, выполняемой на упомянутом охраняемом содержимом упомянутым по меньшей мере одним БГО, то упомянутое программное приложение либо устройство предупреждается об этом различии.

73. По меньшей мере один машиночитаемый носитель данных по п.63, дополнительно содержащий средство для повторного шифрования упомянутого содержимого упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки перед упомянутым выведением упомянутым средством для выведения; средство для дешифрирования упомянутого повторно зашифрованного содержимого по меньшей мере вторым устройством криптографической обработки во внешнем вычислительном устройстве.

RU 2004110622 A

RU 2004110622 A

74. По меньшей мере один машиночитаемый носитель данных по п.73, в котором упомянутое внешнее вычислительное устройство представляет собой либо (A) монитор, либо (B) телеприставку, либо (C) устройство визуализации цифровой обработки сигналов (ЦОС).

75. По меньшей мере один машиночитаемый носитель данных по п.63, в котором зашифрованные текстуры и зашифрованные внеэкранные поверхности, доставленные упомянутым программным приложением либо устройством, кодируются блоковыми шифрами, а упомянутое программное приложение либо устройство смешивает эти блоковые шифры с заранее определенным форматом смешивания, который преобразует местоположение (x,y) в содержимом в сдвиг по меньшей мере для YUV, RGB, YUY2 и упакованного планарного форматов.

76. По меньшей мере один машиночитаемый носитель данных по п.63, в котором по меньшей мере один командный буфер, переданный в блок видео декодера по меньшей мере одного БГО соответственно упомянутому запрашиванию упомянутым средством для запрашивания, зашифровывается упомянутым программным приложением либо устройством и дешифрируется упомянутым блоком видео декодера при осуществлении связи с упомянутым блоком криптографической обработки.

77. По меньшей мере один машиночитаемый носитель данных по п.63, содержащий далее средство для обнаружения несанкционированного доступа к упомянутому по меньшей мере одному командному буферу либо (A) с помощью двух проходов перед использованием по меньшей мере одного командного буфера, либо (B) после того, как командный буфер использован.

78. По меньшей мере одно из операционной системы, машиночитаемого носителя данных с сохраненными на нем множеством исполняемых компьютером команд, сопроцессорное устройство, вычислительное устройство и модулированный сигнал данных, несущий исполняемые компьютером команды для выполнения способа по п.63.

79. Вычислительное устройство, содержащее средство для криптографической защиты охраняемого содержимого в связи с достоверной графической системой вычислительного устройства, причем эта достоверная графическая система имеет видеопамять, по меньшей мере один блок графической обработки (БГО) и устройство криптографической обработки, соединенное для осуществления связи с упомянутым по меньшей мере одним БГО, содержащее средство для запрашивания графической системы программным приложением либо устройством выполнить обработку либо визуализацию охраняемого содержимого, при этом упомянутое средство для запрашивания включает в себя средство для передачи сеансового ключа упомянутым программным приложением либо устройством в графическую систему и средство для передачи упомянутого охраняемого содержимого по меньшей мере в одну зашифрованную часть видеопамяти; средство для дешифрирования содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти упомянутым по меньшей мере одним БГО при осуществлении связи с упомянутым устройством криптографической обработки; средство для выполнения по меньшей мере обработки или визуализации упомянутого дешифрированного содержимого по меньшей мере одним БГО; средство для выведения упомянутого содержимого по меньшей мере из одного БГО.

80. Вычислительное устройство по п.79, в котором, если выход упомянутого средства для выведения отличается от охраняемого содержимого в упомянутом средстве для запрашивания, настроенном для любой обработки, выполняемой на упомянутом охраняемом содержимом упомянутым по меньшей мере одним БГО, то упомянутое программное приложение либо устройство предупреждается об этом различии.

81. Вычислительное устройство по п.79, в котором упомянутое средство для передачи включает в себя средство для передачи упомянутого охраняемого содержимого по меньшей мере к одной зашифрованной поверхности, которая перекрывает по меньшей мере одну первичную поверхность упомянутой видеопамяти.

82. Вычислительное устройство по п.79, в котором упомянутое средство для дешифрирования содержимого упомянутой по меньшей мере одной зашифрованной части

RU 2004110622 A

RU 2004110622 A

видеопамяти включает в себя средство для дешифрирования геометрической части первичной поверхности, благодаря чему пикселы иные, чем в геометрической части, не дешифрируются.

83. Вычислительное устройство по п.79, в котором криптографический процессор постоянно связан с графическим адаптером либо (A) добавлением этого криптографического процессора к существующей микросхеме, либо (B) добавлением этого криптографического процессора в качестве отдельной микросхемы к графическому адаптеру, при этом физическое соединение между криптографическим процессором и остальной частью графического адаптера недоступно и не показывается.

84. Вычислительное устройство по п.81, в котором упомянутое средство для дешифрирования включает в себя средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности механизмом дешифрирования упомянутого БГО, соединенного для осуществления связи с упомянутым устройством криптографической обработки.

85. Вычислительное устройство по п.81, в котором упомянутое средство для дешифрирования включает в себя либо (A) средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности во время выполнения аппаратурой цифроаналогового преобразования (ЦАП) в графической системе, по мере того как содержимое выводится согласно упомянутому выведению, либо (B) средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности во время выполнения непосредственно перед тем, как содержимое достигнет аппаратуры ЦАП в графической системе.

86. Вычислительное устройство по п.81, в котором упомянутое средство для дешифрирования включает в себя средство для дешифрирования упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности перед тем, как содержимое достигнет аппаратуры ЦАП в графической системе, компонентом, не имеющим обратного канала к главной компьютерной системе.

87. Вычислительное устройство по п.79, дополнительно содержащее средство для повторного шифрования упомянутого содержимого упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки перед упомянутым выведением упомянутым средством для выведения; средство для дешифрирования упомянутого повторно зашифрованного содержимого по меньшей мере вторым устройством криптографической обработки во внешнем вычислительном устройстве.

88. Вычислительное устройство по п.79, в котором содержимое передается в цифровом виде к внешнему устройству, имеющему второе устройство криптографической обработки, а упомянутое дешифрирование упомянутого средства для дешифрирования осуществляется в упомянутом внешнем устройстве.

89. Вычислительное устройство по п.87, в котором упомянутое внешнее вычислительное устройство представляет собой либо (A) монитор, либо (B) телеприставку, либо (C) устройство визуализации цифровой обработки сигналов (ЦОС).

90. Вычислительное устройство по п.81, в котором упомянутое средство для передачи включает в себя средство для передачи упомянутого охраняемого содержимого либо (A) к первому зашифрованному конфиденциальному оверлею для базовой визуализации охраняемого содержимого и (B) ко второму зашифрованному защищенному оверлею, специально спроектированному для существующих чувствительных пользовательских интерфейсов, либо (C) к первой зашифрованной области первичной поверхности для базовой визуализации охраняемого содержимого и (D) ко второй зашифрованной области первичной поверхности, специально спроектированной для существующих чувствительных пользовательских интерфейсов.

91. Вычислительное устройство по п.79, в котором упомянутое средство для дешифрирования включает в себя средство для вычисления криптографического дайджеста дешифрированных данных, а упомянутые исполняемые компьютером модули дополнительно содержат средство для передачи упомянутого криптографического

RU 2004110622 A

RU 2004110622 A

дайджеста к программному приложению либо устройству, чтобы гарантировать, что отображенные пикселы являются пикселами, переданными в связи с упомянутым запрашиванием от программного приложения либо устройства через упомянутое средство для запрашивания.

92. Вычислительное устройство по п.90, в котором упомянутый второй зашифрованный защищенный оверлей находится всегда наверху и не закрывается, и содержимое второго зашифрованного защищенного оверлея проверяется упомянутым по меньшей мере одним БГО.

93. Вычислительное устройство по п.90, в котором упомянутое средство для дешифрирования включает в себя либо (A) средство для дешифрирования содержимого первого зашифрованного конфиденциального оверлея первым компонентом дешифрирования потокового шифра, либо (B) средство для дешифрирования содержимого второго зашифрованного защищенного оверлея вторым компонентом дешифрирования потокового шифра, либо (C) средство для дешифрирования содержимого первой зашифрованной области первичной поверхности первым компонентом дешифрирования потокового шифра, либо (D) средство для дешифрирования содержимого второй зашифрованной области первичной поверхности вторым компонентом дешифрирования потокового шифра.

94. Вычислительное устройство по п.93, в котором по меньшей мере один бит каждого пиксела в первичной поверхности используется для определения членства в виртуальной защищенной поверхности для этого пиксела, причем графический адаптер выбирает подходящий ключ дешифрирования для пиксела на основании упомянутого по меньшей мере одного бита.

95. Вычислительное устройство по п.94, в котором, если упомянутый по меньшей мере один бит содержит нулевое значение, то виртуальная защищенная поверхность, связанная с упомянутым по меньшей мере одним битом, интерпретируется как область, не подлежащая дешифрированию.

96. Вычислительное устройство по п.93, дополнительно содержащее средство для выбора, когда доступны дешифрированные пиксельные значения, компонентом выбора пиксела в упомянутом по меньшей мере одном БГО пиксельного значения либо (A) второго зашифрованного защищенного оверлея, либо (B) первого зашифрованного конфиденциального оверлея, либо (3) первичной поверхности.

97. Вычислительное устройство по п.90, в котором упомянутое запрашивание упомянутого средства для запрашивания включает в себя по меньшей мере (A) ограничивающую источник или место назначения рамку упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности, (B) целевой цветовой код упомянутой по меньшей мере одной зашифрованной перекрывающейся поверхности, (C) в случае первого зашифрованного конфиденциального оверлея, описание ключевого указателя шифрования содержимого оверлейного обратного буфера, в который должны отражаться данные, (D) в случае второго зашифрованного защищенного оверлея, описание ячейки памяти, куда записывается по меньшей мере одно из циклического избыточного кода (ЦИК), меры целостности и значения дайджеста дешифрированного содержимого оверлея, (E) ограничивающую источник или место назначения рамку по меньшей мере одной зашифрованной первичной поверхности, и (F) целевой цветовой код упомянутой по меньшей мере одной зашифрованной первичной поверхности.

98. Вычислительное устройство по п.97, в котором программное приложение либо устройство вычисляет по меньшей одно из циклического избыточного кода (ЦИК), меры целостности и значения дайджеста, если упомянутое программное приложение либо устройство имеет отношение к целостности содержимого.

99. Вычислительное устройство по п.79, в котором по меньшей мере один командный буфер, переданный в блок видео декодера по меньшей мере одного БГО соответственно упомянутому запрашиванию, зашифровывается упомянутым программным приложением либо устройством и дешифрируется упомянутым блоком видео декодера при осуществлении связи с упомянутым блоком криптографической обработки.

RU 2004110622 A

RU 2004110622 A

100. Вычислительное устройство по п.99, дополнительно содержащее средство для обнаружения несанкционированного доступа к упомянутому по меньшей мере одному командному буферу либо (A) с помощью двух проходов перед использованием по меньшей мере одного командного буфера, либо (B) после того, как командный буфер использован.

101. Вычислительное устройство, содержащее исполняемые компьютером модули, в том числе исполняемые компьютером команды для криптографической защиты охраняемого содержимого в связи с достоверной графической системой вычислительного устройства, причем эта достоверная графическая система имеет видеопамять, по меньшей мере один блок графической обработки (БГО) и устройство криптографической обработки, соединенное для осуществления связи с упомянутым по меньшей мере одним БГО, содержащее средство для запрашивания графической системы программным приложением либо устройством выполнить обработку либо визуализацию охраняемого содержимого, при этом упомянутое средство для запрашивания включает в себя средство для передачи сеансового ключа упомянутым программным приложением либо устройством в графическую систему для проверки устройством криптографической обработки и для передачи упомянутого охраняемого содержимого по меньшей мере в одну зашифрованную часть видеопамяти; средство для дешифрирования содержимого упомянутой по меньшей мере одной зашифрованной части видеопамяти механизмом дешифрирования входного блока в упомянутом по меньшей мере одним БГО, при этом упомянутый механизм дешифрирования осуществляет связь с упомянутым устройством криптографической обработки; средство для выполнения по меньшей мере обработки или визуализации упомянутого дешифрированного содержимого по меньшей мере одним БГО; средство для шифрования упомянутого содержимого механизмом шифрования-дешифрирования выходного блока по меньшей мере в одном БГО; средство для выведения упомянутого зашифрованного содержимого по меньшей мере из одного БГО.

102. Вычислительное устройство по п.101, в котором упомянутый входной блок является блоком отображения текстуры, а упомянутый выходной блок является блоком альфа-канала, и при этом упомянутая по меньшей мере одна зашифрованная часть упомянутой видеопамяти является зашифрованной текстурной поверхностью.

103. Вычислительное устройство по п.101, в котором упомянутое охраняемое содержимое является либо текстурными данными, либо открытым текстом, либо видео макроблоками.

104. Вычислительное устройство по п.101, в котором упомянутые средство для шифрования и средство для дешифрирования включают в себя, соответственно, средство для шифрования и средство для дешифрирования с помощью блоковых шифров.

105. Вычислительное устройство по п.102, в котором упомянутый механизм дешифрирования блока отображения текстуры дешифрирует заполнение строки кэш-памяти, и механизм шифрования-дешифрирования блока альфа-канала осуществляет шифрование перед записью.

106. Вычислительное устройство по п.102, дополнительно содержащее далее средство для дешифрирования механизмом шифрования-дешифрирования блока альфа-канала при считывании строки кэш-памяти из цветового буфера в видеопамяти.

107. Вычислительное устройство по п.101, дополнительно содержащее средство для отражения упомянутого зашифрованного выходного содержимого из зашифрованной задней первичной поверхности в зашифрованную переднюю первичную поверхность упомянутой видеопамяти; второе средство для дешифрирования упомянутого зашифрованного выходного содержимого вторым механизмом дешифрирования упомянутого по меньшей мере одного БГО при осуществлении связи с упомянутым устройством криптографической обработки; второе средство для выведения упомянутого выходного содержимого.

108. Вычислительное устройство по п.101, в котором упомянутое средство для выведения включает в себя средство для выведения зашифрованного содержимого в цепочку, отражающую конфиденциальный оверлей, а исполняемые компьютером модули дополнительно включают в себя средство для отражения упомянутого зашифрованного

RU 2004110622 A

RU 2004110622 A

выходного содержимого из зашифрованной задней конфиденциальной поверхности в зашифрованную переднюю конфиденциальную поверхность, в соответствии с чем упомянутое шифрование упомянутым механизмом шифрования-дешифрирования включает в себя средство для шифрования, использующее шифрование потоковым шифром; второе средство для дешифрирования упомянутого зашифрованного выходного содержимого механизмом дешифрирования потокового шифра в упомянутом по меньшей мере одном БГО при осуществлении связи с упомянутым устройством криптографической обработки.

109. Вычислительное устройство по п.108, содержащее далее средство для кодирования местоположения в содержимом перед упомянутым шифрованием упомянутым средством для шифрования; средство для декодирования этого местоположения в содержимом после упомянутого второго дешифрирования упомянутым вторым средством для дешифрирования, благодаря чему упомянутое местоположение является недоступным извне, сохраняя целостность преобразования открытого текста в зашифрованный текст.

110. Вычислительное устройство по п.101, в котором, если выход упомянутого средства для выведения отличается от охраняемого содержимого упомянутого средства для запрашивания, настроенного для любой обработки, выполняемой на упомянутом охраняемом содержимом упомянутым по меньшей мере одним БГО, то упомянутое программное приложение либо устройство предупреждается об этом различии.

111. Вычислительное устройство по п.101, причем исполняемые компьютером модули дополнительно включают в себя средство для повторного шифрования упомянутого содержимого упомянутым по меньшей мере одним БГО при осуществлении связи с устройством криптографической обработки перед упомянутым выведением упомянутым средством для выведения; средство для дешифрирования упомянутого повторно зашифрованного содержимого по меньшей мере вторым устройством криптографической обработки во внешнем вычислительном устройстве.

112. Вычислительное устройство по п.111, в котором упомянутое внешнее вычислительное устройство представляет собой либо (A) монитор, либо (B) телеприставку, либо (C) устройство визуализации цифровой обработки сигналов (ЦОС).

113. Вычислительное устройство по п.101, в котором зашифрованные текстуры и зашифрованные внеэкранные поверхности, доставленные упомянутым программным приложением либо устройством, кодируются блоковыми шифрами, а упомянутое программное приложение либо устройство смешивает эти блоковые шифры с заранее определенным форматом смешивания, который преобразует местоположение (x,y) в содержимом в сдвиг по меньшей мере для YUV, RGB, YUY2 и упакованного планарного форматов.

114. Вычислительное устройство по п.101, в котором по меньшей мере один командный буфер, переданный в блок видео декодера по меньшей мере одного БГО соответственно упомянутому запрашиванию упомянутым средством для запрашивания, зашифровывается упомянутым программным приложением либо устройством и дешифрируется упомянутым блоком видео декодера при осуществлении связи с упомянутым блоком криптографической обработки.

115. Вычислительное устройство по п.101, причем исполняемые компьютером модули дополнительно содержат средство для обнаружения несанкционированного доступа к упомянутому по меньшей мере одному командному буферу либо (A) с помощью двух проходов перед использованием по меньшей мере одного командного буфера, либо (B) после того, как командный буфер использован.

RU 2004110622 A

RU 2004110622 A