(19) Евразийское патентное ведомство

(11) 035157 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2020.05.06

(21) Номер заявки
201891890

(22) Дата подачи заявки
2017.03.21

(51) Int. Cl. ***H04N 21/2347*** (2011.01)
H04N 21/254 (2011.01)
H04N 21/8358 (2011.01)
H04N 21/4627 (2011.01)
H04L 29/06 (2006.01)
G06F 21/16 (2013.01)
G06F 21/10 (2013.01)

(54) СПОСОБ УПРАВЛЕНИЯ ЦИФРОВЫМИ ПРАВАМИ НА МУЛЬТИМЕДИА-СОДЕРЖИМОЕ, КЛИЕНТ УПРАВЛЕНИЯ ЦИФРОВЫМИ ПРАВАМИ И СЕРВЕРНАЯ СТОРОНА УПРАВЛЕНИЯ ЦИФРОВЫМИ ПРАВАМИ

(31) **201610185037.5**
(32) **2016.03.29**
(33) **CN**
(43) **2019.03.29**
(86) **PCT/CN2017/077552**
(87) **WO 2017/167077 2017.10.05**

(71)(73) Заявитель и патентовладелец:
АКАДЕМИ ОФ БРОДКАСТИНГ САЙЭНС, СТЭЙТ АДМИНИСТРЕЙШН ОФ ПРЕСС, ПАБЛИКЭЙШН, РЭДИО, ФИЛМ ЭНД ТЕЛЕВИЖН (CN)

(72) Изобретатель:
Ван Лэй, Го Сяося, Го Пэюй, Си Янь, Шэнь Ян (CN)

(74) Представитель:
Левчук Д.В., Ловцов С.В., Коптева Т.В., Вилесов А.С., Ясинский С.Я. (RU)

(56) CN-A-103841469
CN-A-101350918
CN-A-1873652
CN-A-101719205
US-A1-2005066353

(57) Настоящее изобретение относится к способу управления цифровыми правами (DRM) мультимедиа-содержимого, к клиенту DRM, серверной стороне DRM, терминальному устройству и серверу DRM. Способ управления цифровыми правами (DRM) предусматривает прием клиентом DRM запроса на вызов мультимедийного приложения и извлечение уникального идентификатора мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов; отправку запроса авторизации DRM на серверную сторону DRM для получения единицы выполнения авторизации содержимого, при этом запрос авторизации DRM содержит идентификатор мультимедиа-содержимого и базовую информацию клиента DRM; и выполнение единицы выполнения авторизации содержимого в выполняемой среде клиента DRM с тем, чтобы получить функцию авторизации DRM. За счет технического решения согласно настоящему изобретению может быть обеспечена гибкая защита мультимедиа-содержимого и тем самым повышена степень безопасности мультимедиа-содержимого.

035157 B1

035157 B1

Область техники, к которой относится настоящее изобретение

Настоящее изобретение относится к технологиям управления цифровыми правами (DRM), более конкретно к способу DRM для мультимедиа-содержимого, клиенту DRM, серверной стороне DRM, терминальному устройству и серверу DRM.

Предшествующий уровень техники настоящего изобретения

В настоящее время интеллектуальные устройства, к которым относятся телевизоры, используются в домах повсеместно и все чаще становятся для пользователей в повседневной жизни главным источником мультимедиа-содержимого, такого как аудио- и видеоматериалы и документы. Международные поставщики содержимого во главе с поставщиками содержимого из Голливуда активно развертывают операцию по внедрению мультимедиа-содержимого в формате сверхвысокой четкости с разрешением 4K. Японский телевизионный канал NHK добился выхода на уровень промышленного производства устройств кодирования и отображения содержимого с разрешением 8K. Основные поставщики содержимого для домашнего просмотра, такие как телевизионные каналы CCTV и "Цзянсу ТВ", активно занимаются развертыванием производства, транслирования и функционирования мультимедиа-содержимого сверхвысокой четкости. Для прямой трансляции обратного отсчета до Нового года канал "Цзянсу ТВ" использует режим сверхвысокой четкости, что служит подтверждением наступления новой эры мультимедиа-содержимого сверхвысокой четкости. Мультимедиа-содержимое сверхвысокой четкости имеет высокие производственные издержки и стоимость, а также считается следующим этапом развития в медиаиндустрии. Также основные поставщики содержимого для домашнего просмотра, поставщики содержимого из Голливуда и т.п. уделяют особое внимание защите мультимедиа-содержимого сверхвысокой четкости. Для передачи мультимедиа-содержимого сверхвысокой четкости необходимо соблюдать высокие требования к защите прав, а также необходимо обеспечить частую замену алгоритмов защиты содержимого для повышения уровня безопасности. Поэтому крайне необходимо создать технологию защиты содержимого для обеспечения технической поддержки и гарантии для построения работоспособной экосистемы мультимедиа-содержимого сверхвысокой четкости.

В рамках существующей технологии управления цифровыми правами (DRM) цифровое мультимедиа-содержимое обычно находится в зашифрованном и инкапсулированном состоянии. В соответствии с бизнес-правилами, установленными операторами, информация, такая как ключ шифрования содержимого и полномочия для DRM (например, разрешение на получение доступа к содержимому и условия ограничения) инкапсулирована в лицензию авторизации содержимого в соответствии с определенной грамматикой. Лицензия авторизации содержимого отправляется клиенту DRM через взаимодействие между клиентом DRM и серверной стороной DRM терминального устройства, и клиент DRM расшифровывает и воспроизводит содержимое согласно правилам, установленным в разрешении и условиях ограничения, указанных в лицензии авторизации содержимого.

Однако существующая система, работающая по технологии DRM, не в состоянии задать персонализированный алгоритм шифрования содержимого, правило авторизации и т.п. для мультимедиа-содержимого, в результате чего мультимедиа-содержимое находится под слабой защитой. В соответствии с существующей технологией DRM при необходимости внести изменения в алгоритм шифрования содержимого, правило авторизации и т.п. система серверной стороны DRM и система клиента DRM должны обновляться одновременно, а в соответствии с требованиями коммерческой эксплуатации и требованиями к безопасности алгоритм шифрования содержимого, правило авторизации и т.п. не могут гибко изменяться в режиме реального времени, что не способствует интенсивной защите безопасности мультимедиа-содержимого.

В случае с доверенной средой выполнения основные функции клиента DRM, такие как расшифровывание и декодирование, должны исполняться в доверенной среде выполнения. При обновлении клиента DRM также необходимо одновременно обновить всю доверенную среду выполнения, что может отрицательно повлиять на нормальную работу других функций в доверенной среде выполнения, не связанных с DRM.

Кроме того, способ анализа и выполнения разрешения и условий ограничения из существующей лицензии авторизации содержимого необязателен для клиента DRM, поэтому в выполнении легко появляются лазейки. Например, это может быть лазейка, при которой клиент DRM не расшифровывает и не воспроизводит содержимое в соответствии с требованиями разрешения и условий ограничения.

Краткое раскрытие настоящего изобретения

Одной из целей настоящего изобретения является предоставление нового технического решения для управления цифровыми правами, которое сможет решить по меньшей мере одну из указанных выше технических проблем.

В соответствии с первым аспектом настоящего изобретения предлагается способ управления цифровыми правами (DRM) мультимедиа-содержимого, выполняемый в терминальном устройстве, на котором установлен клиент DRM. Способ предусматривает следующие стадии:

стадия 1: прием клиентом DRM запроса на вызов мультимедийного приложения терминального устройства и извлечение клиентом DRM уникального идентификатора мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов;

стадия 2: отправка клиентом DRM на серверную сторону DRM запроса авторизации DRM для извлечения единицы выполнения авторизации содержимого, при этом запрос авторизации DRM содержит идентификатор мультимедиа-содержимого и базовую информацию клиента DRM и серверная сторона DRM генерирует единицу выполнения авторизации содержимого следующим способом: серверная сторона DRM получает алгоритм шифрования содержимого и ключ шифрования содержимого, применяемые для мультимедиа-содержимого, и полномочия DRM клиента DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM посредством запроса, а затем она генерируется в соответствии с идентификатором мультимедиа-содержимого алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информации клиента DRM и полномочий DRM клиента DRM для мультимедиа-содержимого;

стадия 3: выполнение клиентом DRM единицы выполнения авторизации содержимого в выполняемой среде клиента DRM, проверка соответствия выполняемой среды терминала полномочиям DRM клиента DRM для мультимедиа-содержимого через единицу выполнения авторизации содержимого и в случае соответствия расшифровывание мультимедиа-содержимого в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого.

Необязательно единица выполнения авторизации содержимого выдается клиенту DRM после подписания серверной стороной DRM. После извлечения единицы выполнения авторизации содержимого клиент DRM сначала проверяет подпись единицы выполнения авторизации содержимого, а затем в случае положительного результата проверки выполняет единицу выполнения авторизации содержимого.

Необязательно на стадии 2 клиент DRM выполняет единицу выполнения обмена данными в выполняемой среде клиента DRM и отправляет запрос авторизации DRM на серверную сторону DRM через единицу выполнения обмена данными.

Необязательно между стадией 1 и стадией 2 способ дополнительно предусматривает стадию извлечения единицы выполнения обмена данными: отправку клиентом DRM запроса на единицу выполнения обмена данными на серверную сторону DRM для извлечения единицы выполнения обмена данными. Запрос на единицу выполнения обмена данными содержит базовую информацию клиента DRM. Единица выполнения обмена данными генерируется серверной стороной DRM в соответствии с базовой информацией клиента DRM.

Необязательно единица выполнения обмена данными выдается клиенту DRM после подписания серверной стороной DRM. После извлечения единицы выполнения обмена данными клиент DRM сначала проверяет подпись единицы выполнения обмена данными, а затем в случае положительного результата проверки выполняет единицу выполнения обмена данными.

Необязательно полномочия DRM клиента DRM для мультимедиа-содержимого содержат указания, что при воспроизведении мультимедиа-содержимого клиент DRM должен проверить цифровой водяной знак мультимедиа-содержимого. Единица выполнения авторизации содержимого уведомляет клиента DRM выполнить единицу выполнения цифрового водяного знака. Клиент DRM выполняет единицу выполнения цифрового водяного знака в выполняемой среде клиента DRM, проверяет цифровой водяной знак, внедренный в мультимедиа-содержимое в процессе воспроизведения мультимедиа-содержимого посредством единицы выполнения цифрового водяного знака и в случае отрицательного результата проверки останавливает воспроизведение мультимедиа-содержимого. Единица выполнения цифрового водяного знака поступает от серверной стороны DRM на клиент DRM, запрашивающий в соответствии с уведомлением единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому.

Необязательно цифровой водяной знак мультимедиа-содержимого содержит информацию о требовании ограничения, наложенном поставщиком мультимедиа-содержимого для среды воспроизведения мультимедиа-содержимого. Единица выполнения цифрового водяного знака определяет, соответствует ли выполняемая среда терминала требованию ограничения, наложенному поставщиком мультимедиа-содержимого на среду воспроизведения мультимедиа-содержимого, в процессе воспроизведения мультимедиа-содержимого и в случае несоответствия останавливает воспроизведение мультимедиа-содержимого.

Необязательно полномочия DRM клиента DRM для мультимедиа-содержимого содержат указания, что клиент DRM должен внедрить цифровой водяной знак для отслеживания мультимедиа-содержимого при воспроизведении мультимедиа-содержимого. Единица выполнения авторизации содержимого уведомляет клиента DRM выполнить единицу выполнения цифрового водяного знака. Клиент DRM выполняет единицу выполнения цифрового водяного знака в выполняемой среде клиента DRM и внедряет цифровой водяной знак для отслеживания мультимедиа-содержимого в процессе воспроизведения мультимедиа-содержимого посредством единицы выполнения цифрового водяного знака. Единица выполнения цифрового водяного знака поступает от серверной стороны DRM на клиент DRM, запрашивающий в соответствии с уведомлением единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому.

Необязательно единица выполнения цифрового водяного знака выдается клиенту DRM после подписания серверной стороной DRM. После извлечения единицы выполнения цифрового водяного знака

клиент DRM сначала проверяет подпись единицы выполнения цифрового водяного знака, а затем в случае положительного результата проверки выполняет единицу выполнения цифрового водяного знака.

Необязательно выполняемая среда клиента DRM содержит ядро единицы выполнения и модуль адаптации операционной системы терминала. Клиент DRM выполняет единицу выполнения посредством ядра единицы выполнения и адаптирует ядро единицы выполнения к операционной системе терминала посредством модуля адаптации операционной системы терминала.

Необязательно ядро единицы выполнения предоставляет интерфейс управления памятью, внешний интерфейс управления хранением, интерфейс сетевого управления, интерфейс алгоритма шифрования, интерфейс контроля воспроизведения и интерфейс управления выводом данных для выполнения единицы выполнения. Клиент DRM адаптирует интерфейс управления памятью, внешний интерфейс управления хранением, интерфейс сетевого управления, интерфейс алгоритма шифрования, интерфейс контроля воспроизведения и интерфейс управления выводом данных ядра единицы выполнения к соответствующим интерфейсам операционной системы терминала посредством модуля адаптации операционной системы терминала.

Необязательно выполняемая среда клиента DRM дополнительно содержит модуль управления и планирования единицы выполнения. Клиент DRM планирует различные единицы управления и управляет ими посредством модуля управления и планирования единицы выполнения, что предусматривает внесение в ядро единицы выполнения плана касательно единицы выполнения для выполнения, добавления, удаления и обновления единицы выполнения.

В соответствии со вторым аспектом настоящего изобретения предлагается способ управления цифровыми правами (DRM) мультимедиа-содержимого, выполняемый на серверной стороне DRM. Способ предусматривает следующие стадии:

стадия 1: прием серверной стороной DRM запроса авторизации DRM, отправленного клиентом DRM, при этом запрос авторизации DRM содержит уникальный идентификатор мультимедиа-содержимого и базовую информацию клиента DRM;

стадия 2: получение серверной стороной DRM алгоритма шифрования содержимого и ключа шифрования содержимого, применяемых для мультимедиа-содержимого, и полномочий DRM клиента DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM посредством запроса;

стадия 3: генерирование серверной стороной DRM единицы выполнения авторизации содержимого в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемых для мультимедиа-содержимого, базовой информацией клиента DRM и полномочиями DRM клиента DRM для мультимедиа-содержимого, при этом единица выполнения авторизации содержимого выполнена с возможностью выполнения в выполняемой среде клиента DRM таким образом, чтобы проверять, соответствует ли выполняемая среда терминала терминального устройства, где расположен клиент DRM, полномочиям DRM клиента DRM для мультимедиа-содержимого, и в случае соответствия расшифровывать мультимедиа-содержимое в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого;

стадия 4: выдача серверной стороной DRM сгенерированной единицы выполнения авторизации содержимого клиенту DRM.

Необязательно между стадией 3 и стадией 4 способ дополнительно предусматривает стадию подписания сгенерированной единицы выполнения авторизации содержимого серверной стороной DRM.

Необязательно на стадии 3 серверная сторона DRM выполняет поиск шаблона единицы выполнения авторизации содержимого, соответствующего мультимедиа-содержимому, в соответствии с идентификатором мультимедиа-содержимого или алгоритмом шифрования содержимого, применяемым для мультимедиа-содержимого; или запрос авторизации DRM дополнительно содержит номер версии DRM, соответствующий мультимедиа-содержимому, и серверная сторона DRM выполняет поиск шаблона единицы выполнения авторизации содержимого, соответствующего мультимедиа-содержимому, в соответствии с номером версии DRM, соответствующим мультимедиа-содержимому. Серверная сторона DRM генерирует единицу выполнения авторизации содержимого по шаблону единицы выполнения авторизации содержимого, полученному по результатам поиска.

Необязательно стадия планирования единицы выполнения цифрового водяного знака указана в шаблоне единицы выполнения авторизации содержимого, соответствующем мультимедиа-содержимому. Серверная сторона DRM принимает запрос клиента DRM на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому. Клиент DRM генерирует запрос клиента DRM на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, в соответствии со стадией планирования единицы выполнения цифрового водяного знака единицей выполнения авторизации содержимого. Серверная сторона DRM выполняет поиск шаблона единицы выполнения цифрового водяного знака, соответствующего мультимедиа-содержимому, в соответствии с идентификатором мультимедиа-содержимого и генерирует единицу выполнения цифрового водяного знака по шаблону единицы выполнения цифрового водяного знака, полученному по результатам поиска. Серверная сторона DRM выдает сгенерированную единицу выполнения цифрового водяного знака клиенту DRM.

Необязательно на стадии 2 серверная сторона DRM получает алгоритм шифрования и ключ шифро-

вания содержимого, которые применяются для мультимедиа-содержимого, от системы управления ключами посредством запроса в соответствии с идентификатором мультимедиа-содержимого.

Необязательно на стадии 2 серверная сторона DRM получает полномочия DRM клиента DRM для мультимедиа-содержимого от системы операционной поддержки посредством запроса в соответствии с идентификатором мультимедиа-содержимого и базовой информацией клиента DRM.

В соответствии с третьим аспектом настоящего изобретения предлагается клиент DRM, расположенный в терминальном устройстве, на котором установлена интеллектуальная операционная система. Клиент DRM содержит интерфейс мультимедийного приложения, модуль извлечения единицы выполнения и единицу выполнения авторизации содержимого, где

интерфейс мультимедийного приложения выполнен с возможностью получения запроса на вызов мультимедийного приложения терминального устройства и извлечения уникального идентификатора мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов;

модуль извлечения единицы выполнения выполнен с возможностью отправки запроса авторизации DRM на серверную сторону DRM для извлечения единицы выполнения авторизации содержимого, при этом запрос авторизации DRM содержит идентификатор мультимедиа-содержимого и базовую информацию клиента DRM; и

единица выполнения авторизации содержимого выполнена с возможностью проверки соответствия выполняемой среды терминала полномочиям DRM клиента DRM для мультимедиа-содержимого и в случае соответствия расшифровки мультимедиа-содержимого в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого, при этом

серверная сторона DRM генерирует единицу выполнения авторизации содержимого следующим способом: серверная сторона DRM получает алгоритм шифрования содержимого и ключ шифрования содержимого, применяемые для мультимедиа-содержимого, и полномочия DRM клиента DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM посредством запроса, а затем она генерируется в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информации клиента DRM и полномочий DRM клиента DRM для мультимедиа-содержимого.

Необязательно клиент DRM дополнительно содержит модуль проверки подписи единицы выполнения, выполненный с возможностью проверки подписи единицы выполнения авторизации содержимого.

Необязательно полномочия DRM клиента DRM для мультимедиа-содержимого содержат указания, что при воспроизведении мультимедиа-содержимого клиент DRM должен проверить цифровой водяной знак мультимедиа-содержимого. Клиент DRM дополнительно содержит единицу выполнения цифрового водяного знака. Единица выполнения авторизации содержимого дополнительно выполнена с возможностью отправки на модуль извлечения единицы выполнения уведомления об извлечении единицы выполнения цифрового водяного знака. Модуль извлечения единицы выполнения дополнительно выполнен с возможностью отправки запроса на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, от серверной стороны DRM в соответствии с уведомлением. Единица выполнения цифрового водяного знака выполнена с возможностью проверки цифрового водяного знака, внедренного в мультимедиа-содержимое, в процессе воспроизведения мультимедиа-содержимого и остановки воспроизведения мультимедиа-содержимого в случае отрицательного результата проверки.

Необязательно цифровой водяной знак мультимедиа-содержимого содержит информацию о требовании ограничения, наложенном поставщиком мультимедиа-содержимого для среды воспроизведения мультимедиа-содержимого. Единица выполнения цифрового водяного знака дополнительно выполнена с возможностью определения, соответствует ли выполняемая среда терминала требованию ограничения, наложенному поставщиком мультимедиа-содержимого на среду воспроизведения мультимедиа-содержимого, в процессе воспроизведения мультимедиа-содержимого, и в случае несоответствия останавливается воспроизведение мультимедиа-содержимого.

Необязательно полномочия DRM клиента DRM для мультимедиа-содержимого содержат указания, что клиент DRM должен внедрить цифровой водяной знак для отслеживания мультимедиа-содержимого при воспроизведении мультимедиа-содержимого. Клиент DRM дополнительно содержит единицу выполнения цифрового водяного знака. Единица выполнения авторизации содержимого дополнительно выполнена с возможностью отправки на модуль извлечения единицы выполнения уведомления об извлечении единицы выполнения цифрового водяного знака. Модуль извлечения единицы выполнения дополнительно выполнен с возможностью отправки запроса на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, от серверной стороны DRM в соответствии с уведомлением. Единица выполнения цифрового водяного знака выполнена с возможностью внедрения цифрового водяного знака для отслеживания мультимедиа-содержимого в процессе воспроизведения мультимедиа-содержимого.

Необязательно клиент DRM дополнительно содержит ядро единицы выполнения и модуль адаптации операционной системы терминала. Ядро единицы выполнения выполнено с возможностью выполнения единицы выполнения. Модуль адаптации операционной системы терминала выполнен с возможностью адаптации ядра единицы выполнения к операционной системе терминала.

Необязательно ядро единицы выполнения выполнено с возможностью предоставления интерфейса управления памятью, внешнего интерфейса управления хранением, интерфейса сетевого управления, интерфейса алгоритма шифрования, интерфейса контроля воспроизведения и интерфейса управления выводом данных для выполнения единицы выполнения. Модуль адаптации операционной системы терминала выполнен с возможностью адаптации интерфейса управления памятью, внешнего интерфейса управления хранением, интерфейса сетевого управления, интерфейса алгоритма шифрования, интерфейса контроля воспроизведения и интерфейса управления выводом данных ядра единицы выполнения к соответствующим интерфейсам операционной системы терминала.

Необязательно клиент DRM дополнительно содержит модуль управления и планирования единицы выполнения. Модуль управления и планирования единицы выполнения выполнен с возможностью планирования и управления различными единицами выполнения и предусматривает внесение в ядро единицы выполнения плана касательно единицы выполнения для выполнения, добавления, удаления и обновления единицы выполнения.

В соответствии с четвертым аспектом настоящего изобретения предлагается серверная сторона DRM, содержащая модуль приема сообщений DRM, модуль извлечения информации DRM, связанной с мультимедиа-содержимым, модуль генерирования единицы выполнения и модуль выдачи единицы выполнения, при этом

модуль приема сообщений DRM выполнен с возможностью приема запроса авторизации DRM, отправленного клиентом DRM, причем запрос авторизации DRM содержит уникальный идентификатор мультимедиа-содержимого и базовую информацию клиента DRM;

модуль извлечения информации DRM, связанной с мультимедиа-содержимым, выполнен с возможностью получения алгоритма шифрования содержимого и ключа шифрования содержимого, применяемых для мультимедиа-содержимого, и полномочий DRM клиента DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM посредством запроса;

модуль генерирования единицы выполнения выполнен с возможностью генерирования единицы выполнения авторизации содержимого в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информацией клиента DRM и полномочиями DRM клиента DRM для мультимедиа-содержимого и в соответствии с шаблоном единицы выполнения авторизации содержимого, соответствующим мультимедиа-содержимому, при этом единица выполнения авторизации содержимого выполнена с возможностью выполнения в выполняемой среде клиента DRM таким образом, чтобы проверять, соответствует ли выполняемая среда терминала терминального устройства, где расположен клиент DRM, полномочиям DRM клиента DRM для мультимедиа-содержимого, и в случае соответствия расшифровывать мультимедиа-содержимое в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого; и

модуль выдачи единицы выполнения выполнен с возможностью выдачи единицы выполнения авторизации содержимого на клиент DRM.

Необязательно серверная сторона DRM дополнительно содержит модуль подписи единицы выполнения, выполненный с возможностью подписания единицы выполнения авторизации содержимого до того, как модуль выдачи единицы выполнения выдаст единицу выполнения авторизации содержимого.

Необязательно серверная сторона DRM дополнительно содержит модуль управления шаблоном единицы выполнения, выполненный с возможностью управления шаблоном единицы выполнения авторизации содержимого, предусматривающий добавление, обновление и удаление шаблона выполнения авторизации содержимого.

Необязательно серверная сторона DRM дополнительно содержит интерфейс управления ключами. Модуль извлечения информации мультимедиа-содержимого DRM выполнен с возможностью обмена данными с системой управления ключами через интерфейс управления ключами и получения алгоритма шифрования содержимого и ключа шифрования содержимого, которые применяются для мультимедиа-содержимого, от системы управления ключами в соответствии с идентификатором мультимедиа-содержимого посредством запроса.

Необязательно серверная сторона DRM дополнительно содержит интерфейс операционной поддержки.

Модуль извлечения информации мультимедиа-содержимого DRM дополнительно выполнен с возможностью обмена данными с системой операционной поддержки через интерфейс операционной поддержки и получения полномочий DRM клиента DRM для мультимедиа-содержимого от системы операционной поддержки в соответствии с идентификатором мультимедиа-содержимого и базовой информации клиента DRM посредством запроса.

В соответствии с пятым аспектом настоящего изобретения предлагается клиент DRM, расположенный в терминальном устройстве, на котором установлена интеллектуальная операционная система. Клиент DRM содержит интерфейс мультимедийного приложения, модуль управления и планирования единицы выполнения, ядро единицы выполнения и модуль адаптации операционной системы терминала, где

интерфейс мультимедийного приложения выполнен с возможностью получения запроса на вызов

мультимедийного приложения терминального устройства и извлечения уникального идентификатора мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов;

модуль управления и планирования единицы выполнения выполнен с возможностью поиска единицы выполнения, соответствующей мультимедиа-содержимому, в соответствии с запросом на вызов и запуска ядра единицы выполнения для выполнения единицы выполнения с тем, чтобы осуществить авторизацию DRM для мультимедиа-содержимого; и если единица выполнения, соответствующая мультимедиа-содержимому, не будет найдена, отправки сообщения DRM на серверную сторону DRM для извлечения единицы выполнения, соответствующей мультимедиа-содержимому, проверки подписи извлеченной единицы выполнения для определения допустимости единицы выполнения с последующим запуском ядра единицы выполнения DRM для выполнения единицы выполнения с тем, чтобы осуществить авторизацию DRM для мультимедиа-содержимого; и

модуль адаптации операционной системы терминала выполнен с возможностью осуществления адаптации ядра единицы выполнения DRM и операционной системы терминала.

Необязательно ядро единицы выполнения выполнено с возможностью предоставления интерфейса управления памятью, внешнего интерфейса управления хранением, интерфейса сетевого управления, интерфейса алгоритма шифрования, интерфейса контроля воспроизведения и интерфейса управления выводом данных для выполнения единицы выполнения. Модуль адаптации операционной системы терминала выполнен с возможностью адаптации интерфейса управления памятью, внешнего интерфейса управления хранением, интерфейса сетевого управления, интерфейса алгоритма шифрования, интерфейса контроля воспроизведения и интерфейса управления выводом данных ядра единицы выполнения к соответствующим интерфейсам операционной системы терминала.

В соответствии с шестым аспектом настоящего изобретения предлагается серверная сторона DRM, содержащая модуль обработки сообщения DRM, модуль управления шаблоном единицы выполнения, шаблон единицы выполнения и модуль генерирования единицы выполнения, где

модуль обработки сообщения DRM выполнен с возможностью приема сообщения DRM, отправленного клиентом DRM, при этом сообщение DRM содержит идентификатор мультимедиа-содержимого и базовую информацию клиента DRM; выбора соответствующего шаблона единицы выполнения в соответствии с сообщением DRM и вызова модуля генерирования единицы выполнения для генерирования единицы выполнения в соответствии с выбранным шаблоном единицы выполнения, при этом единица выполнения выполнена с возможностью выполнения на выполняемой среде клиента DRM с тем, чтобы осуществлять авторизацию DRM для мультимедиа-содержимого; подписания единицы выполнения, сгенерированной модулем генерирования единицы выполнения; и выдачи подписанной единицы выполнения клиенту DRM;

модуль управления шаблоном единицы выполнения выполнен с возможностью управления шаблоном единицы выполнения.

Необязательно шаблон единицы выполнения содержит шаблон единицы выполнения авторизации содержимого. Модуль обработки сообщения DRM выполнен с возможностью вызова модуля генерирования единицы выполнения для генерирования единицы выполнения авторизации содержимого в соответствии с идентификатором мультимедиа-содержимого, алгоритма шифрования содержимого и ключа шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информации клиента DRM и полномочий DRM клиента DRM для мультимедиа-содержимого и в соответствии с выбранным шаблоном единицы выполнения авторизации содержимого. Единица выполнения авторизации содержимого выполнена с возможностью выполнения в выполняемой среде клиента DRM с тем, чтобы проверять, соответствует ли выполняемая среда терминала терминального устройства, где расположен клиент DRM, полномочиям DRM клиента DRM для мультимедиа-содержимого, и в случае соответствия расшифровывать мультимедиа-содержимое в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого.

Необязательно серверная сторона DRM дополнительно содержит интерфейс управления ключами и интерфейс операционной поддержки. Модуль обработки сообщения DRM дополнительно выполнен с возможностью обмена данными с системой управления ключами через интерфейс управления ключами и получения алгоритма шифрования и ключа шифрования содержимого, соответствующих мультимедиа-содержимому, от системы управления ключами в соответствии с идентификатором мультимедиа-содержимого посредством запроса. Модуль обработки сообщения DRM дополнительно выполнен с возможностью обмена данными с системой операционной поддержки через интерфейс операционной поддержки и получения полномочий DRM клиента DRM для мультимедиа-содержимого от системы операционной поддержки в соответствии с идентификатором мультимедиа-содержимого и базовой информацией клиента DRM посредством запроса.

В соответствии с седьмым аспектом настоящего изобретения также предлагается терминальное устройство, содержащее клиент DRM согласно любому из предыдущих аспектов.

Необязательно клиент DRM выполняется в интеллектуальной операционной системе терминального устройства или выполняется в доверенной среде выполнения терминального устройства.

В соответствии с восьмым аспектом настоящего изобретения также предлагается сервер DRM, со-

держащий серверную сторону DRM согласно любому из предыдущих аспектов.

В соответствии с настоящим изобретением способ авторизации содержимого посредством лицензии авторизации содержимого изменен, клиент DRM запрашивает авторизацию DRM для мультимедиа-содержимого от серверной стороны DRM после приема запроса на вызов мультимедийного приложения, серверная сторона DRM генерирует единицу выполнения авторизации содержимого в соответствии с алгоритмом шифрования и ключом шифрования содержимого мультимедиа-содержимого, полномочия DRM клиента DRM для мультимедиа-содержимого и т.п. и выдает единицу выполнения авторизации содержимого клиенту DRM, и клиент DRM непосредственно выполняет единицу выполнения авторизации содержимого в выполняемой среде клиента DRM с тем, чтобы расшифровать мультимедиа-содержимое. За счет применения технического решения согласно настоящему изобретению может быть обеспечена гибкая защита мультимедиа-содержимого и тем самым повышена степень безопасности мультимедиа-содержимого.

Другие признаки и преимущества настоящего изобретения станут более понятными после ознакомления с приведенными в качестве примера вариантами осуществления настоящего изобретения, описанными подробно со ссылками на прилагаемые фигуры.

Краткое описание фигур

Прилагаемые фигуры составляют часть настоящего описания, а также иллюстрируют варианты осуществления настоящего изобретения и вместе с описанием помогают изложить его основные идеи.

На фиг. 1 показана блок-схема системы выполнения мультимедиа-содержимого в соответствии с вариантом осуществления настоящего изобретения;

на фиг. 2 показана схема стадий способа управления цифровыми правами в соответствии с первым вариантом осуществления настоящего изобретения;

на фиг. 3 показана структурная схема клиента DRM и серверной стороны DRM в соответствии с первым вариантом осуществления настоящего изобретения;

на фиг. 4 показана структурная схема клиента DRM и серверной стороны DRM в соответствии со вторым вариантом осуществления настоящего изобретения;

на фиг. 5 показана структурная схема клиента DRM и серверной стороны DRM в соответствии с четвертым вариантом осуществления настоящего изобретения; и

на фиг. 6 показана структурная схема терминального устройства в соответствии с вариантом осуществления настоящего изобретения.

Подробное раскрытие настоящего изобретения

Далее варианты осуществления настоящего изобретения будут описаны со ссылкой на прилагаемые фигуры. Следует отметить, что относительное расположение компонентов и стадий, числовые выражения и числовые значения, приведенные в контексте этих вариантов осуществления, не ограничивают объем настоящего изобретения, если это специально не указано.

Приведенное далее описание по меньшей мере одного приведенного в качестве примера варианта осуществления является иллюстративным и никоим образом не ограничивает объем изобретения, его реализацию или применение.

Методы, способы и устройства, известные специалисту в области техники настоящего изобретения, могут быть описаны в общем, однако там, где это требуется, методы, способы и устройства должны рассматриваться как часть описания.

Во всех примерах, приведенных в настоящем документе, любые конкретные значения следует толковать исключительно как приведенные в качестве примера и не рассматривать их как ограничения. Поэтому в других примерах, приведенных в качестве примера вариантов осуществления могут фигурировать другие значения.

Следует отметить, что на фигурах одинаковыми цифровыми и буквенными позициями обозначены одинаковые элементы, поэтому после первого определения на фигуре такие элементы не будут дополнительно описываться в контексте последующих фигур.

В соответствии с настоящим изобретением предлагается решение для управления цифровыми правами мультимедиа-содержимого, и оно относится к серверной стороне DRM, предоставляющей сервис DRM и клиента DRM пользовательского терминального устройства.

Терминальное устройство представляет собой интеллектуальное электронное устройство, такое как компьютер, смартфон и планшет, с установленной интеллектуальной операционной системой (такой как Android, WINDOWS и IOS).

Клиент DRM образован выполняемой средой клиента DRM и единицей выполнения. Единица выполнения представляет собой объект, генерируемый серверной стороной DRM в соответствии требованием клиента DRM, и который может быть выполнен в выполняемой среде клиента DRM, такой как программа, инструкция, команда и код. Под выполняемой средой клиента DRM следует понимать внутреннюю выполняемую среду, предоставленную клиентом 100 DRM для единицы выполнения.

Единица выполнения выполняется в выполняемой среде клиента DRM и внешне не находится в непосредственном контакте с клиентом DRM, а контакт с операционной системой терминала обеспечивается выполняемой средой клиента DRM.

Клиент DRM осуществляет обоснованную авторизацию для мультимедиа-содержимого посредством выполнения единицы выполнения в выполняемой среде клиента DRM. Единицы выполнения в соответствии с настоящим изобретением включают, кроме прочего, единицу выполнения обмена данными, единицу выполнения авторизации содержимого, единицу выполнения цифрового водяного знака и т.п.

Система выполнения мультимедиа-содержимого в соответствии с вариантом осуществления настоящего изобретения показана на фиг. 1, а технический результат, достигаемый настоящим изобретением, описан в целом.

Система 4 управления содержимым отправляет мультимедиа-содержимое, которое должно воспроизводиться, в систему 3 шифрования содержимого для шифрования. Система 3 шифрования содержимого шифрует мультимедиа-содержимое, затем отправляет зашифрованное мультимедиа-содержимое в систему 6 операционной поддержки для ожидания воспроизведения по требованию пользователя, отправляет ключ шифрования содержимого в систему 5 управления ключами для управления хранением и отправляет базовую информацию мультимедиа-содержимого на сервер 2 DRM для хранения. Базовая информация мультимедиа-содержимого, по меньшей мере, должна содержать уникальный идентификатор мультимедиа-содержимого и также может содержать другую информацию мультимедиа-содержимого, такую как имя документа, размер, длительность и соответствующий номер версии DRM. Система 3 шифрования содержимого может дополнительно отправлять алгоритм шифрования, используемый для шифрования мультимедиа-содержимого, в систему 5 управления ключами и/или на сервер 2 DRM для хранения. Под ключом шифрования содержимого в соответствии с настоящим изобретением следует понимать ключ для шифрования ключа содержимого, и шифрование мультимедиа-содержимого осуществляется с помощью ключа содержимого.

Серверная сторона 200 DRM может генерировать шаблон единицы выполнения авторизации содержимого с помощью алгоритма шифрования мультимедиа-содержимого, или шаблон единицы выполнения авторизации содержимого на серверной стороне 200 DRM может быть выдан на сервер 2 DRM системой 3 шифрования содержимого или системой 6 операционной поддержки.

Шаблон единицы выполнения авторизации содержимого выполнен с возможностью генерирования единицы выполнения авторизации содержимого, которая может выполняться непосредственно в выполняемой среде клиента DRM. Единица выполнения авторизации содержимого может передавать информацию авторизации клиента DRM оператору IF, который определяет, соответствует ли выполняемая среда терминала правилу авторизации DRM, например необходимо проверить локальный сертификат терминального устройства, и мультимедиа-содержимое будет расшифровано и воспроизведено только в случае положительного результата проверки, и т.п. Шаблон единицы выполнения авторизации содержимого может быть задан специалистом в области техники настоящего изобретения различными способами, которые не будут описаны в настоящем документе. Серверная сторона 200 DRM может дополнительно содержать другие типы шаблонов единицы выполнения, такие как шаблон единицы выполнения обмена данными и шаблон единицы выполнения цифрового водяного знака. Новые типы шаблонов могут быть заданы в соответствии с операционными потребностями.

Интеллектуальная операционная система 11, мультимедийное приложение 12 и клиент 100 DRM выполняются в терминальном устройстве 1. Мультимедийное приложение 11, например, представляет собой проигрыватель мультимедиа или мультимедийное приложение. Пользователь может воспроизвести мультимедиа-содержимое по запросу с помощью мультимедийного приложения 11. Кроме того, пользователь также может купить или скачать мультимедиа-содержимое через мультимедийное приложение 11. Мультимедийное приложение 11 извлекает мультимедиа-содержимое с помощью системы 6 операционной поддержки и предоставляет мультимедиа-содержимое пользователю.

Когда пользователь запрашивает мультимедиа-содержимое через мультимедийное приложение 11 в системе 6 операционной поддержки, мультимедийное приложение 11 извлекает уникальный идентификатор мультимедиа-содержимого из системы 6 операционной поддержки и также может извлекать такую информацию, как номер версии DRM, соответствующий мультимедиа-содержимому, и адрес серверной стороны DRM. Затем мультимедийное приложение 11 вызывает клиента 100 DRM для выполнения таких операций, как авторизация DRM для мультимедиа-содержимого, с тем, чтобы воспроизвести мультимедиа-содержимое.

После вызова мультимедийным приложением 11 клиент 100 DRM отправляет сообщение DRM на серверную сторону 200 DRM. После приема сообщения DRM серверная сторона 200 DRM выбирает в соответствии с сообщением DRM соответствующий шаблон единицы выполнения для генерирования единицы выполнения и выдает единицу выполнения клиенту 100 DRM. Клиент 100 DRM выполняет единицу выполнения в выполняемой среде клиента DRM и осуществляет авторизацию для мультимедиа-содержимого посредством выполнения единицы выполнения. Сообщение DRM в соответствии с настоящим изобретением содержит, кроме прочего, запрос авторизации DRM, а также может быть запросом для единицы выполнения обмена данными и т.п.

Серверная сторона 200 DRM может заменить шаблон единицы выполнения в соответствии с операционными потребностями. Единица выполнения, сгенерированная в соответствии с шаблоном единицы выполнения, может быть выполнена непосредственно в выполняемой среде клиента DRM после ее от-

правки клиенту 100 DRM. При необходимости добавить новую функцию DRM или новое правило авторизации необходимо только добавить новый шаблон единицы выполнения на серверной стороне 2 DRM.

Клиент 100 DRM может выполняться в интеллектуальной операционной системе терминального устройства 1 и также может выполняться в доверенной среде выполнения терминального устройства 1. Когда клиент 100 DRM выполняется в доверенной среде выполнения терминала, если необходимо обновить алгоритм шифрования содержимого и т.п., необходимо только сгенерировать новый шаблон выполнения авторизации содержимого на серверной стороне 200 DRM, серверная сторона 200 DRM генерирует единицу выполнения авторизации содержимого в соответствии с новым шаблоном выполнения авторизации содержимого, а затем отправляет единицу выполнения авторизации содержимого клиенту 100 DRM для выполнения, тем самым избегая проблем, связанных с частым обновлением клиента 100 DRM.

Первый вариант осуществления

Способ управления цифровыми правами, клиент 100 DRM и серверная сторона 200 DRM, предоставленные в соответствии с первым вариантом осуществления настоящего изобретения, показаны на фиг. 2 и 3. Клиент 100 DRM содержит интерфейс 101 мультимедийного приложения, модуль 108 извлечения единицы выполнения, модуль 109 проверки подписи единицы выполнения, ядро 106 единицы выполнения, а модуль 107 адаптации операционной системы терминала и модуль управления и планирования единицы выполнения (не показан на фигурах). Серверная сторона 200 DRM содержит интерфейс 205 операционной поддержки, интерфейс 206 управления ключами, модуль 207 приема сообщений DRM, модуль 208 извлечения информации DRM, связанной с мультимедиа-содержимым, модуль 204 генерирования единицы выполнения, модуль 210 подписи единицы выполнения, модуль 209 выдачи единицы выполнения и модуль 203 управления шаблоном единицы выполнения.

Стадия S101 предусматривает прием клиентом 100 DRM запроса на вызов мультимедийного приложения терминального устройства через интерфейс 101 мультимедийного приложения и извлечение клиентом 100 DRM базовой информации мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов. Базовая информация мультимедиа-содержимого, по меньшей мере, должна содержать уникальный идентификатор мультимедиа-содержимого и также может содержать другую информацию мультимедиа-содержимого, такую как имя документа, размер, длительность и соответствующий номер версии DRM.

Стадия S102 предусматривает отправку клиентом 100 DRM запроса авторизации DRM на серверную сторону 200 DRM посредством модуля 108 извлечения единицы выполнения, при этом запрос авторизации DRM должен, по меньшей мере, содержать идентификатор мультимедиа-содержимого и базовую информацию клиента 100 DRM и также может содержать информацию о номере версии DRM, соответствующую мультимедиа-содержимому. Базовая информация клиента 100 DRM должна, по меньшей мере, содержать идентификатор клиента 100 DRM и также может содержать другую информацию клиента 100 DRM, такую как информация об адресе, номер версии и сертификат.

Стадия S103 предусматривает прием серверной стороной 200 DRM запроса авторизации DRM посредством модуля 207 приема сообщений DRM; получение модулем 208 извлечения информации DRM, связанной с мультимедиа-содержимым, алгоритма шифрования содержимого и ключа шифрования содержимого, применяемых для мультимедиа-содержимого, и полномочия DRM клиента 100 DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM; генерирование модулем 204 генерирования единицы выполнения единицы 104 выполнения авторизации содержимого в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информации клиента 100 DRM и полномочий DRM клиента 100 DRM для мультимедиа-содержимого; и, наконец, выдачу модулем 209 выдачи единицы выполнения сгенерированной единицы 104 выполнения авторизации содержимого клиенту 100 DRM.

Стадия S104 предусматривает прием с помощью клиента 100 DRM единицы 104 выполнения авторизации содержимого посредством модуля 108 извлечения единицы выполнения, выполнение единицы 104 выполнения авторизации содержимого в выполняемой среде клиента DRM, проверку соответствия выполняемой среды терминала полномочиям DRM клиента 100 DRM для мультимедиа-содержимого через единицу 104 выполнения авторизации содержимого и в случае соответствия расшифровывание мультимедиа-содержимого в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого и контроль воспроизведения мультимедиа-содержимого. Например, полномочия DRM клиента 100 DRM для мультимедиа-содержимого предполагают, что в период времени с 20:00 до 12:00 клиент DRM может только расшифровать и воспроизвести мультимедиа-содержимое, единица 104 выполнения авторизации содержимого будет определять, находится ли выполняемая среда терминала в промежутке между 20:00 и 12:00, и если выполняемая среда терминала отвечает ограничивающему условию, с 20:00 до 12:00, единица 104 выполнения авторизации содержимого расшифровывает мультимедиа-содержимое и контролирует воспроизведение мультимедиа-содержимого.

Для еще большего повышения безопасности мультимедиа-содержимого на стадии S103 после генерирования модулем 204 генерирования единицы выполнения единицы выполнения авторизации содержимого сначала модуль 210 подписи единицы выполнения подписывает единицу выполнения авториза-

ции содержимого, а затем модуль 209 выдачи единицы выполнения выдает клиенту DRM подписанную единицу выполнения авторизации содержимого. На стадии S104 после извлечения единицы 104 выполнения авторизации содержимого клиент DRM сначала проверяет подпись единицы 104 выполнения авторизации содержимого, а затем в случае положительного результата проверки выполняет единицу 104 выполнения авторизации содержимого в выполняемой среде клиента DRM.

Модуль 204 генерирования единицы выполнения может осуществлять поиск шаблона единицы выполнения авторизации содержимого, соответствующего мультимедиа-содержимому, в соответствии с идентификатором мультимедиа-содержимого и/или алгоритмом шифрования содержимого, применяемыми для мультимедиа-содержимого и/или номера версии DRM, соответствующих мультимедиа-содержимому, и генерирует единицу 104 выполнения авторизации содержимого по шаблону единицы выполнения авторизации содержимого, полученному по результатам поиска.

Модуль 108 извлечения единицы выполнения клиента 100 DRM также может представлять собой единицу выполнения обмена данными. После извлечения запроса на вызов мультимедийного приложения клиент 100 DRM отправляет серверной стороне 200 DRM запрос единицы выполнения обмена данными. Запрос единицы выполнения обмена данными должен, по меньшей мере, содержать базовую информацию клиента 100 DRM и может также содержать идентификатор мультимедиа-содержимого и информацию о номере версии DRM, соответствующую мультимедиа-содержимому. После приема модулем 207 приема сообщений DRM запроса клиента 100 DRM на единицу выполнения обмена данными модуль 204 генерирования единицы выполнения выполняет поиск шаблона единицы выполнения обмена данными в соответствии с запросом единицы выполнения обмена данными и генерирует единицу выполнения обмена данными в соответствии с шаблоном единицы выполнения обмена данными, полученным по результатам поиска. Модуль 210 подписи единицы выполнения подписывает единицу выполнения обмена данными, сгенерированную модулем 204 генерирования единицы выполнения. Модуль 209 выдачи единицы выполнения выдает подписанную единицу выполнения обмена данными клиенту 100 DRM. После получения единицы выполнения обмена данными клиент 100 DRM сначала проверяет подпись единицы выполнения обмена данными, а затем, в случае положительного результата проверки, выполняет единицу выполнения обмена данными в выполняемой среде клиента DRM. Модуль 204 генерирования единицы выполнения может осуществлять поиск шаблона единицы выполнения обмена данными в соответствии с идентификатором мультимедиа-содержимого и/или номером версии DRM, соответствующим мультимедиа-содержимому и/или базовой информации клиента DRM.

Серверная сторона 200 DRM может дополнительно содержать модуль 203 управления шаблоном единицы выполнения для управления шаблоном единицы выполнения, предусматривая скачивание, добавление, обновление и удаление шаблона единицы выполнения.

Модуль 208 извлечения информации DRM, связанной с мультимедиа-содержимым, выполнен с возможностью обмена данными с системой управления ключами через интерфейс 206 управления ключами и получения алгоритма шифрования и ключа шифрования содержимого, применяемых для мультимедиа-содержимого, от системы управления ключами в соответствии с идентификатором мультимедиа-содержимого посредством запроса, или модуль 208 извлечения информации DRM, связанной с мультимедиа-содержимым, получает алгоритм шифрования содержимого мультимедиа-содержимого из области хранения сервера 2 DRM.

Модуль 208 извлечения информации DRM, связанной с мультимедиа-содержимым, обменивается данными с системой операционной поддержки через интерфейс 205 операционной поддержки и получает полномочия DRM клиента DRM для мультимедиа-содержимого от системы операционной поддержки в соответствии с идентификатором мультимедиа-содержимого и базовой информацией клиента DRM посредством запроса.

Выполняемая среда клиента DRM содержит ядро 106 единицы выполнения, модуль 107 адаптации операционной системы и модуль управления и планирования единицы выполнения. Клиент 100 DRM планирует различные единицы управления и управляет ими посредством модуля управления и планирования единицы выполнения, что предусматривает внесение в ядро 106 единицы выполнения плана касательно единицы выполнения для выполнения, добавления, удаления и обновления единицы выполнения. Клиент 100 DRM адаптирует ядро 106 единицы выполнения к операционной системе терминала посредством модуля 107 адаптации операционной системы терминала. Ядро 106 единицы выполнения дополнительно содержит интерфейс управления памятью, внешний интерфейс управления хранением, интерфейс сетевого управления, интерфейс алгоритма шифрования, интерфейс контроля воспроизведения и интерфейс управления выводом данных для выполнения единицы выполнения. Модуль 107 адаптации операционной системы терминала адаптирует интерфейс управления памятью, внешний интерфейс управления хранением, интерфейс сетевого управления, интерфейс алгоритма шифрования, интерфейс контроля воспроизведения и интерфейс управления выводом данных ядра 106 единицы выполнения к соответствующим интерфейсам операционной системы терминала.

Второй вариант осуществления

Способ управления цифровыми правами, клиент 100 DRM и серверная сторона 200 DRM, предоставленные в соответствии со вторым вариантом осуществления настоящего изобретения, показаны на

фиг. 4. В соответствии со вторым вариантом осуществления на основании первого варианта осуществления добавляется функция цифрового водяного знака. Более конкретно, если цифровой водяной знак внедрен в мультимедиа-содержимое, которое должно воспроизводиться, полномочия DRM клиента 100 DRM для мультимедиа-содержимого предусматривают, что клиент 100 DRM должен проверять цифровой водяной знак мультимедиа-содержимого при воспроизведении мультимедиа-содержимого. Стадия планирования единицы выполнения цифрового водяного знака указана в шаблоне единицы выполнения авторизации содержимого, соответствующем мультимедиа-содержимому.

Когда единица 104 выполнения авторизации содержимого выполняется в выполняемой среде клиента DRM и уведомляет клиента 100 DRM, что единица выполнения цифрового водяного знака должна быть запущена, модуль 108 извлечения единицы выполнения запрашивает у серверной стороны 200 DRM единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, в соответствии с уведомлением. Запрос на единицу выполнения цифрового водяного знака может содержать идентификатор мультимедиа-содержимого и базовую информацию клиента 100 DRM.

После приема серверной стороной 200 DRM запроса клиента 100 DRM на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, модуль 204 генерирования единицы выполнения выполняет поиск шаблона единицы выполнения цифрового водяного знака, соответствующего мультимедиа-содержимому, в соответствии с идентификатором мультимедиа-содержимого и генерирует единицу выполнения цифрового водяного знака в соответствии с шаблоном единицы выполнения цифрового водяного знака, соответствующим мультимедиа-содержимому. Затем модуль 210 подписи единицы выполнения подписывает единицу выполнения цифрового водяного знака. Модуль 209 выдачи единицы выполнения выдает подписанную единицу 105 выполнения цифрового водяного знака клиенту 100 DRM.

После приема клиентом 100 DRM единицы 105 выполнения цифрового водяного знака модуль 109 проверки подписи единицы выполнения сначала проверяет подпись единицы 105 выполнения цифрового водяного знака. В случае положительного результата проверки единица 105 выполнения цифрового водяного знака выполняется в выполняемой среде клиента DRM. Единица 105 выполнения цифрового водяного знака проверяет цифровой водяной знак, внедренный в мультимедиа-содержимое, в процессе воспроизведения мультимедиа-содержимого и останавливает воспроизведение мультимедиа-содержимое в случае отрицательного результата проверки.

Кроме того, если цифровой водяной знак мультимедиа-содержимого содержит информацию о требовании ограничения поставщика мультимедиа-содержимого для среды воспроизведения мультимедиа-содержимого, единица 105 выполнения цифрового водяного знака определяет соответствие выполняемой среды терминала требованию ограничения поставщика мультимедиа-содержимого для среды воспроизведения мультимедиа-содержимого в процессе воспроизведения мультимедиа-содержимого и в случае несоответствия останавливает воспроизведение мультимедиа-содержимого. Поставщик содержимого в соответствии с настоящим изобретением может быть оригинальным поставщиком содержимого. Например, если кинокомпания отвечает за съемку фильма, кинокомпания является оригинальным поставщиком содержимого и может выдвигать специальные требования к среде воспроизведения снятого ею фильма. Например, если кинокомпания требует, чтобы фильм воспроизводился на смарт-телевизорах, а не на смартфонах, кинокомпания может внедрить в фильм цифровой водяной знак, содержащий информацию о требовании ограничения для среды воспроизведения. Оператор предоставляет фильм пользователям после покупки полномочий на демонстрацию фильма. Перед просмотром фильма пользователи могут расшифровать и воспроизвести фильм, только если они выполнят требования кинокомпании для среды воспроизведения, а также выполнят требования DRM оператора, которые он выдвигает к фильму.

Третий вариант осуществления

Способ управления цифровыми правами, клиент 100 DRM и серверная сторона 200 DRM, предоставленные в соответствии с третьим вариантом осуществления настоящего изобретения, показаны на фиг. 4. В соответствии с третьим вариантом осуществления на основании первого варианта осуществления добавляется функция цифрового водяного знака. Более конкретно, полномочия DRM клиента DRM для мультимедиа-содержимого содержат указания, что клиент DRM должен внедрить цифровой водяной знак для отслеживания мультимедиа-содержимого при воспроизведении мультимедиа-содержимого. Стадия планирования единицы выполнения цифрового водяного знака указана в шаблоне единицы выполнения авторизации содержимого, соответствующем мультимедиа-содержимому.

Когда единица 104 выполнения авторизации содержимого выполняется в выполняемой среде клиента DRM и уведомляет клиента 100 DRM, что единица выполнения цифрового водяного знака должна быть запущена, модуль 108 извлечения единицы выполнения запрашивает у серверной стороны 200 DRM единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, в соответствии с уведомлением. Запрос на единицу выполнения цифрового водяного знака может содержать идентификатор мультимедиа-содержимого и базовую информацию клиента 100 DRM.

После приема серверной стороной 200 DRM запроса клиента 100 DRM на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, модуль 204 генерирования единицы выполнения выполняет поиск шаблона единицы выполнения цифрового водяного знака, соот-

ветствующего мультимедиа-содержимому, в соответствии с идентификатором мультимедиа-содержимого и генерирует единицу выполнения цифрового водяного знака в соответствии с шаблоном единицы выполнения цифрового водяного знака, соответствующим мультимедиа-содержимому. Затем модуль 210 подписи единицы выполнения подписывает единицу выполнения цифрового водяного знака. Модуль 209 выдачи единицы выполнения выдает подписанную единицу 105 выполнения цифрового водяного знака клиенту 100 DRM.

После приема клиентом 100 DRM единицы 105 выполнения цифрового водяного знака модуль 109 проверки подписи единицы выполнения сначала проверяет подпись единицы 105 выполнения цифрового водяного знака. Затем в случае положительного результата проверки единица 105 выполнения цифрового водяного знака выполняется в выполняемой среде клиента DRM. Единица 105 выполнения цифрового водяного знака внедряет цифровой водяной знак для отслеживания мультимедиа-содержимого в процессе воспроизведения мультимедиа-содержимого.

В соответствии с другими вариантами осуществления, когда единица 104 выполнения авторизации содержимого уведомляет клиента 100 DRM о том, что единица выполнения цифрового водяного знака должна быть запущена, уведомление может содержать базовую информацию единицы выполнения цифрового водяного знака. Базовая информация единицы выполнения цифрового водяного знака в соответствии с настоящим изобретением, по меньшей мере, содержит идентификатор единицы выполнения цифрового водяного знака, а также может содержать такую информацию, как номер версии цифрового водяного знака. В этом случае, когда модуль 108 извлечения единицы выполнения отправляет запрос на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, от серверной стороны 200 DRM, запрос на единицу выполнения цифрового водяного знака может содержать базовую информацию единицы выполнения цифрового водяного знака и базовую информацию клиента 100 DRM. После приема серверной стороной 200 DRM запроса клиента 100 DRM на единицу выполнения цифрового водяного знака, соответствующую мультимедиа-содержимому, модуль 204 генерирования единицы выполнения выполняет поиск шаблона единицы выполнения цифрового водяного знака в соответствии с базовой информацией единицы выполнения цифрового водяного знака и генерирует единицу выполнения цифрового водяного знака в соответствии с найденным шаблоном единицы выполнения цифрового водяного знака.

Четвертый вариант осуществления

Способ управления цифровыми правами, клиент 100 DRM и серверная сторона 200 DRM, предоставленные в соответствии с четвертым вариантом осуществления настоящего изобретения, показаны на фиг. 5. Клиент 100 DRM содержит интерфейс 1001 мультимедийного приложения, модуль 1002 управления и планирования единицы выполнения, ядро 1006 единицы выполнения и модуль 1007 адаптации операционной системы терминала. Серверная сторона 200 DRM содержит интерфейс 2005 операционной поддержки, интерфейс 2006 управления ключами, модуль 2001 планирования сообщения DRM, модуль 2002 обработки сообщения DRM, модуль 2004 генерирования единицы выполнения и модуль 2003 управления шаблоном единицы выполнения.

Стадия S201 предусматривает прием клиентом 100 DRM запроса на вызов мультимедийного приложения терминального устройства через интерфейс 101 мультимедийного приложения и извлечение клиентом 100 DRM базовой информации мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов. Базовая информация мультимедиа-содержимого, по меньшей мере, должна содержать уникальный идентификатор мультимедиа-содержимого и также может содержать другую информацию мультимедиа-содержимого, такую как имя документа, размер, длительность и соответствующий номер версии DRM.

Стадия S202 предусматривает отправку запроса модулем 1002 управления и планирования единицы выполнения для определения, есть ли доступная единица 1003 выполнения обмена данными в соответствии с идентификатором мультимедиа-содержимого и/или номером версии DRM, соответствующая мультимедиа-содержимому, и в случае наличия планирование выполнения ядром 1006 единицы выполнения DRM единицы 1003 выполнения обмена данными.

Стадия S203 предусматривает отправку единицей 1003 выполнения обмена данными запроса авторизации DRM на серверную сторону 200 DRM, при этом запрос авторизации DRM, по меньшей мере, должен содержать идентификатор мультимедиа-содержимого и базовую информацию клиента 100 DRM, а также может содержать информацию о номере версии DRM, соответствующую мультимедиа-содержимому. Базовая информация клиента 100 DRM должна, по меньшей мере, содержать идентификатор клиента 100 DRM и также может содержать другую информацию клиента 100 DRM, такую как информация об адресе, номер версии и сертификат.

Стадия S204 предусматривает вызов модулем 2001 планирования сообщения DRM серверной стороны 200 DRM определенного модуля 2002 обработки сообщения DRM для обработки запроса авторизации DRM после приема запроса авторизации DRM.

Стадия S205 предусматривает отправку запроса модулем 2002 обработки сообщения DRM на алгоритм шифрования и ключа шифрования содержимого, соответствующих мультимедиа-содержимому, у системы управления ключами в соответствии с идентификатором мультимедиа-содержимого через ин-

терфейс 2006 управления ключами, отправку запроса на полномочия DRM клиента 100 DRM для мультимедиа-содержимого у системы операционной поддержки в соответствии с идентификатором мультимедиа-содержимого и базовой информацией клиента 100 DRM через интерфейс операционной поддержки 2005, и отправку запроса на соответствующий шаблон единицы выполнения авторизации содержимого у модуля 2003 управления шаблоном единицы выполнения DRM в соответствии с идентификатором мультимедиа-содержимого.

Стадия S206 предусматривает отправку модулем 2002 обработки сообщения DRM идентификатора мультимедиа-содержимого, алгоритма шифрования содержимого и ключа шифрования содержимого, применяемых для мультимедиа-содержимого, базовой информации клиента 100 DRM, полномочий DRM клиента 100 DRM для мультимедиа-содержимого и найденного шаблона единицы выполнения авторизации содержимого, на модуль 2004 генерирования единицы выполнения DRM.

Стадия S207 предусматривает генерирование модулем 2004 генерирования единицы выполнения DRM соответствующей единицы выполнения авторизации содержимого в соответствии с найденным шаблоном единицы выполнения авторизации содержимого и в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информации клиента 100 DRM и полномочий DRM клиента 100 DRM для мультимедиа-содержимого.

Стадия S208 предусматривает подписание модулем 2002 обработки сообщения DRM сгенерированной единицы выполнения авторизации содержимого и выдачу подписанной единицы выполнения авторизации содержимого клиенту 100 DRM.

Стадия S209 предусматривает прием клиентом 100 DRM единицы 1004 выполнения авторизации содержимого через единицу 1003 выполнения обмена данными и отправку уведомления единицей 1003 выполнения обмена данными на модуль 1002 управления и планирования единицы выполнения после приема единицы выполнения авторизации содержимого.

Стадия S210 предусматривает сначала проверку модулем 1002 управления и планирования единицы выполнения допустимости подписи единицы 1004 выполнения авторизации содержимого и в случае положительного результата проверки планирования выполнения единицы 1004 выполнения авторизации содержимого ядром 1006 единицы выполнения.

Стадия S211 предусматривает определение и проверку с помощью единицы 1004 выполнения авторизации содержимого соответствия выполняемой среды терминала полномочиям DRM клиента DRM для мультимедиа-содержимого и в случае соответствия расшифровывание ключа шифрования содержимого для получения ключа содержимого, расшифровывание мультимедиа-содержимого в соответствии с ключом содержимого и алгоритмом шифрования содержимого и контроль воспроизведения.

На стадии S202, если модуль 1002 управления и планирования единицы выполнения не находит соответствующую единицу выполнения обмена данными, модуль 1002 управления и планирования единицы выполнения запрашивает единицу выполнения обмена данными у серверной стороны 200 DRM. После приема запроса серверная сторона DRM опрашивает шаблон единицы выполнения обмена данными, генерирует единицу выполнения обмена данными в соответствии с базовой информацией клиента DRM и в соответствии с шаблоном единицы выполнения обмена данными, подписывает единицу выполнения обмена данными и отправляет подписанную единицу выполнения обмена данными клиенту 100 DRM. После того как клиент 100 DRM получает единицу выполнения обмена данными, модуль 1002 управления и планирования единицы выполнения сначала проверяет допустимость подписи единицы выполнения обмена данными, сохраняет единицу выполнения обмена данными после получения успешного результата проверки и взаимодействует с серверной стороной 200 DRM, выполняя единицу выполнения обмена данными с помощью ядра единицы выполнения для извлечения других единиц выполнения, таких как единица выполнения авторизации содержимого.

На фиг. 5 видно, что клиент 100 DRM дополнительно содержит единицу 1005 выполнения цифрового водяного знака. Принцип и функции единицы 1005 выполнения цифрового водяного знака могут быть аналогичны второму и третьему вариантам осуществления. Стадия планирования единицы выполнения цифрового водяного знака указана в шаблоне единицы выполнения авторизации содержимого, соответствующем мультимедиа-содержимому. Клиент 100 DRM генерирует запрос на единицу выполнения цифрового водяного знака в соответствии с выполнением единицы 1004 выполнения авторизации содержимого. Серверная сторона 200 DRM выполняет поиск шаблона единицы выполнения цифрового водяного знака, соответствующего мультимедиа-содержимому, генерирует единицу 1005 выполнения цифрового водяного знака в соответствии с шаблоном и выдает единицу 1005 выполнения цифрового водяного знака клиенту 100 DRM.

Модуль 1002 управления и планирования единицы выполнения отвечает за планирование и управление скачиванием, проверкой, установкой, обновлением, отправкой запросов, выполнением и завершением единицы выполнения и устанавливает и выполняет единицу выполнения, запуская ядро 1006 единицы выполнения.

В соответствии с приведенными выше вариантами осуществления настоящего изобретения также предлагается терминальное устройство с описанным выше клиентом DRM, сервером DRM с описанной

выше серверной стороной DRM.

Терминальное устройство 1 в соответствии с вариантами осуществления настоящего изобретения показано на фиг. 6. Терминальное устройство 1 содержит память 3020 и процессор 3010. Память 3020 выполнена с возможностью хранения команд для контроля процессора 3010 для выполнения соответствующей операции с целью осуществления способа управления цифровыми правами мультимедиа-содержимого согласно настоящему изобретению.

Терминальное устройство 1 дополнительно содержит интерфейсное устройство 3030, устройство 3040 связи, устройство 3050 отображения, устройство 3060 ввода, динамик 3070, микрофон 3080 и т.п.

Процессор 3010, например, может представлять собой центральный процессор (ЦП), микропроцессор (МП) и т.п. Память 3020, например, может представлять собой ПЗУ (постоянное запоминающее устройство), ОЗУ(оперативное запоминающее устройство), энергозависимую память, например жесткий диск. Интерфейсное устройство 3030, например, содержит USB-интерфейс, разъем для наушников и т.п. Устройство 3040 связи, например, может быть выполнено с возможностью осуществления проводного или беспроводного подключения. Устройство 3050 отображения, например, представляет собой жидкокристаллический дисплей, сенсорный дисплей и т.п. Устройство 3060 ввода, например, может включать сенсорный экран, клавиатуру и т.п. Пользователь может вводить и выводить голосовую информацию через динамик 3070 и микрофон 3080.

Терминальное устройство, показанное на фиг. 6, приведено исключительно в качестве примера и никоим образом не ограничивает настоящее изобретение и область его при на то, что на фиг. 6 показано несколько устройств, часть из них может использоваться только в настоящем изобретении. Специалист в области техники настоящего изобретения может разработать команду в соответствии с техническим решением согласно настоящему изобретению. Управление процессором для работы по команде хорошо известно в области техники настоящего изобретения, поэтому подробно не описывается в этом документе.

В настоящем изобретении способ авторизации содержимого посредством лицензии авторизации содержимого изменен. Клиент DRM запрашивает авторизацию DRM для мультимедиа-содержимого у серверной стороны DRM после приема запроса на вызов мультимедийного приложения. Серверная сторона DRM генерирует единицу выполнения авторизации содержимого в соответствии с алгоритмом шифрования и ключом шифрования содержимого мультимедиа-содержимого, полномочий DRM клиента DRM для мультимедиа-содержимого и т.п. и выдает единицу выполнения авторизации содержимого клиенту DRM, и клиент DRM непосредственно выполняет единицу выполнения авторизации содержимого в выполняемой среде клиента DRM с тем, чтобы расшифровать мультимедиа-содержимое.

В соответствии с техническим результатом настоящего изобретения, так как единица выполнения, сгенерированная серверной стороной DRM, может непосредственно выполняться в выполняемой среде клиента DRM после отправки клиенту DRM, для определенного мультимедиа-содержимого персонализированный алгоритм шифрования содержимого, правило авторизации и т.п. может задаваться до тех пор, пока на серверной стороне DRM будет доступен соответствующий шаблон единицы выполнения.

Используя технический результат настоящего изобретения, алгоритм шифрования содержимого может часто обновляться или заменяться, что особенно необходимо для защиты содержимого очень высокой четкости, тем самым исключая проблему частого обновления клиента DRM.

Используя технический результат настоящего изобретения, новая функция DRM или новое правило авторизации может дополнительно добавляться до тех пор, пока на серверной стороне DRM будет доступен соответствующий шаблон единицы выполнения без обновления клиента DRM и все серверной стороны DRM, тем самым упрощая коммерческую операцию.

Очевидно, что с помощью технического результата настоящего изобретения становится возможным гибкое управление и защита мультимедиа-содержимого, и, следовательно, повышается его безопасность.

Клиент DRM в соответствии с настоящим изобретением может выполняться в доверенной среде выполнения терминала. В случае с доверенной средой выполнения для обновления алгоритма защиты содержимого и т.п. необходимо только, чтобы серверная сторона DRM генерировала разные единицы выполнения и отправляла их клиенту DRM для выполнения, что не влияет на нормальную работу функций других не-DRM клиентов в доверенной среде выполнения.

Клиент DRM выполняет единицу выполнения в выполняемой среде клиента DRM и осуществляет авторизацию для мультимедиа-содержимого посредством выполнения единицы выполнения. Единица выполнения выдается серверной стороной DRM. Таким образом, ситуация, при которой клиент DRM не расшифровывает и не воспроизводит содержимое в соответствии с требованиями условий разрешения и ограничения, может быть предотвращена, тем самым могут быть устранены лазейки и недостатки, связанные с существующим способом разбора лицензии авторизации содержимого.

Настоящее изобретение может представлять собой систему, способ и/или компьютерный программный продукт. Компьютерный программный продукт может включать машиночитаемый носитель (или носители) с хранящимися на нем машиночитаемыми программными командами, на основании которых процессор сможет реализовывать аспекты настоящего изобретения.

Машиночитаемый носитель может представлять собой материальное устройство, способное удерживать и хранить команды для использования устройством выполнения команд. Машиночитаемый носи-

тель может представлять собой, например, кроме прочего, электронное запоминающее устройство, магнитное запоминающее устройство, оптическое запоминающее устройство, электромагнитное запоминающее устройство, полупроводниковое запоминающее устройство или любую комбинацию перечисленных устройств. Неисчерпывающий список характерных примеров машиночитаемых носителей включает следующее: портативную машиночитаемую дискету, жесткий диск, оперативное запоминающее устройство (ОЗУ), постоянное запоминающее устройство (ПЗУ), электрически стираемое перепрограммируемое ПЗУ (ЭСППЗУ или флеш-память), статическое оперативное запоминающее устройство (статическое ОЗУ), портативный компакт-диск для однократной записи данных (CD-ROM), универсальный цифровой диск (DVD), флеш-карту, гибкий диск, механически шифрованное устройство, такое как перфокарты или рельефные структуры в канавке с записанными командами, и любую другую комбинацию указанного выше. Машиночитаемый носитель, о котором идет речь в настоящем документе, не следует рассматривать как переходные сигналы как таковые, такие как радиоволны или другие свободно распространяющиеся электромагнитные волны, электромагнитные волны, распространяющиеся через волновод или другую передающую среду (например, световые импульсы, проходящие по оптоволоконному кабелю), или электрические сигналы, передаваемые по кабелю.

Машиночитаемые программные команды, описанные в настоящем документе, могут быть скачаны на соответствующие вычислительные или обрабатывающие устройства с машиночитаемого носителя или на внешний компьютер или внешнее запоминающее устройство по сети, например Интернет, локальной сети, глобальной сети и/или беспроводной сети. Сеть может содержать медные кабели передачи, волокна оптической передачи, беспроводную передачу, роутеры, брандмауэры, коммутационные устройства, шлюзовые компьютеры и/или пограничные серверы. На плату сетевого адаптера или интерфейс сети в каждом вычислительном или обрабатывающем устройстве из сети поступают машиночитаемые программные команды, перенаправляемые для хранения в машиночитаемый носитель в соответствующем вычислительном или обрабатывающем устройстве.

Машиночитаемые программные команды для выполнения операций согласно настоящему изобретению могут представлять собой команды ассемблера, команды архитектуры системы команд (ISA), машинные команды, машинозависимые команды, микрокод, команды встроенного ПО, данные для установки состояния, или исходный код, или объектный код, написанный в любой комбинации на одном или нескольких языках программирования, включая объектно-ориентированный язык программирования, такой как Smalltalk, C++ и т.п., и традиционные процедурные языки программирования, такие как язык программирования "C" или аналогичные языки программирования. Машиночитаемые программные команды могут выполняться полностью на пользовательском компьютере, частично на пользовательском компьютере, как автономный программный пакет, частично на пользовательском компьютере и частично на удаленном компьютере или полностью на удаленном компьютере или сервере. В последнем случае удаленный компьютер может быть подключен к пользовательскому компьютеру через любую сеть, включая локальную сеть (LAN) или глобальную сеть (WAN), или же подключение может быть выполнено с внешним компьютером (например, через Интернет с при помощи интернет-провайдера). В соответствии с некоторыми вариантами осуществления электронная схема, содержащая, например, программируемую логическую схему, программируемые пользователем матрицы логических элементов (FPGA) или программируемую вентильную матрицу (ПВМ), может выполнять машиночитаемые программные команды, используя информацию о состоянии машиночитаемых программных команд для персонализации электронной схемы для выполнения аспектов настоящего изобретения.

Аспекты настоящего изобретения описаны в настоящем документе со ссылками на блок-схемы и/или структурные схемы способов, устройств (систем) и компьютерных программных продуктов в соответствии с вариантами осуществления изобретения. Следует понимать, что каждый блок блок-схем и/или структурных схем, а также комбинации блоков блок-схем и/или структурных схем могут быть реализованы машиночитаемыми программными командами.

Эти машиночитаемые программные команды могут быть предоставлены процессором компьютера общего назначения, специального компьютера или другого устройства обработки программируемых данных для создания машины с тем, чтобы команды, выполняемые через процессор компьютера или другого устройства обработки программируемых данных, создавали средства для осуществления функций/действий, указанных в блоке или блоках блок-схемы и/или структурной схемы. Эти машиночитаемые программные команды также могут храниться в машиночитаемом носителе, который может направлять компьютер, устройство обработки программируемых данных и/или другие устройства для работы определенным образом так, чтобы машиночитаемый носитель с хранящимися в нем командами содержал изделие, содержащее команды, выполняющие аспекты функции/действия, указанного в блоке или блоках блок-схемы и/или структурной схемы.

Машиночитаемые программные команды также могут быть загружены на компьютер, другое устройство обработки программируемых данных или другие устройства для выполнения последовательных рабочих стадий на компьютере, другом программируемом устройстве или другом устройстве для создания выполняемого компьютером способа так, чтобы команды, выполняемые на компьютере, другом программируемом устройстве или другом устройства, выполняли функции/действия, указанные в блоке или

блоках блок-схемы и/или структурной схемы.

Блок-схема и структурные схемы, показанные на фигурах, отображают архитектуру, функционал и принцип действия возможных вариантов систем, способов и компьютерных программных продуктов в соответствии с разными вариантами осуществления настоящего изобретения. В связи с этим каждый блок в блок-схеме или структурных схемах может отвечать модулю, сегменту или части кода, содержащего одну или несколько выполняемых команд для осуществления указанной одной или нескольких логических функций. Также следует отметить, что в некоторых альтернативных вариантах функции, указанные в блоке, могут выполняться в порядке, отличном от того, что указан на фигурах. Например, два блока, показанные последовательно, могут на самом деле выполняться практически одновременно, или же иногда блоки могут выполняться в обратном порядке в зависимости от того, какая функция необходима. Также следует отметить, что каждый блок, указанный в блок-схемах и/или структурных схемах, а также комбинации блоков на блок-схемах и/или структурных схемах, может быть выполнен аппаратными системами специального назначения, которые выполняют указанные функции или действия, или комбинациями аппаратных систем специального назначения и компьютерных команд.

Специалисту в области техники настоящего изобретения хорошо известно, что варианты осуществления с помощью аппаратного осуществления, программного обеспечения или комбинации программного и аппаратного обеспечения могут быть эквиваленты друг другу.

Описание различных вариантов осуществления настоящего изобретения выполнено в иллюстративных и описательных целях, не является исчерпывающим и не ограничивает настоящее изобретение раскрытыми вариантами осуществления. Различные изменения описанных вариантов осуществления будут понятны специалисту в области техники, к которой относится настоящее изобретение, при этом не выходя за пределы объема настоящего изобретения. Терминология, используемая в настоящем документе, была выбрана так, чтобы наилучшим образом объяснить принципы вариантов осуществления, практическое применение или техническое усовершенствование технологий, присутствующих на рынке, или дать возможность другим специалистам в области техники понять раскрытые здесь варианты осуществления. Объем настоящего изобретения определяется в прилагаемой формуле изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ управления цифровыми правами (DRM) мультимедиа-содержимого, осуществляемый в терминальном устройстве, на котором установлен клиент DRM, причем способ предусматривает:

стадия 1: прием клиентом DRM запроса на вызов мультимедийного приложения терминального устройства и извлечение клиентом DRM уникального идентификатора мультимедиа-содержимого, которое должно воспроизводиться, из запроса на вызов;

стадия 2: отправка клиентом DRM на серверную сторону DRM запроса авторизации DRM для извлечения единицы выполнения авторизации содержимого, при этом запрос авторизации DRM содержит идентификатор мультимедиа-содержимого и базовую информацию клиента DRM, при этом

серверная сторона DRM генерирует единицу выполнения авторизации содержимого следующим способом: серверная сторона DRM получает алгоритм шифрования содержимого и ключ шифрования содержимого, применяемые для мультимедиа-содержимого, и полномочия DRM клиента DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM посредством запроса, а затем она генерируется в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемыми для мультимедиа-содержимого, базовой информации клиента DRM и полномочий DRM клиента DRM для мультимедиа-содержимого; и

стадия 3: выполнение клиентом DRM единицы выполнения авторизации содержимого в выполняемой среде клиента DRM, проверка соответствия выполняемой среды терминала полномочиям DRM клиента DRM для мультимедиа-содержимого через единицу выполнения авторизации содержимого и в случае соответствия расшифровывание мультимедиа-содержимого в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого,

причем клиент DRM включает ядро единицы выполнения и модуль управления и планирования единицы выполнения, ядро единицы выполнения выполнено с возможностью выполнения единицы выполнения, а клиент DRM планирует и управляет единицами выполнения посредством модуля управления и планирования единицы выполнения, включая внесение в ядро единицы выполнения плана касательно единицы выполнения для выполнения, а единицы выполнения включают единицу выполнения авторизации содержимого.

2. Способ по п.1, дополнительно включающий стадию проверки подписи единицы выполнения авторизации содержимого посредством модуля проверки подписи единицы выполнения клиента DRM.

3. Способ по п.1 или 2, дополнительно включающий стадию адаптации ядра единицы выполнения к операционной системе терминала посредством модуля адаптации операционной системы терминала клиента DRM.

4. Способ по любому из пп.1-3, дополнительно включающий стадию предоставления посредством ядра единицы выполнения интерфейса управления памятью, внешнего интерфейса управления хранени-

ем, интерфейса сетевого управления, интерфейса алгоритма шифрования, интерфейса контроля воспроизведения и интерфейса управления выводом данных для выполнения единицы выполнения; и

стадию адаптации интерфейса управления памятью, внешнего интерфейса управления хранением, интерфейса сетевого управления, интерфейса алгоритма шифрования, интерфейса контроля воспроизведения и интерфейса управления выводом данных ядра единицы выполнения к соответствующим интерфейсам операционной системы терминала посредством модуля адаптации операционной системы терминала.

5. Способ по любому из пп.1-4, дополнительно включающий стадию планирования и управления различными единицами выполнения, включая внесение в ядро единицы выполнения плана касательно единицы выполнения для выполнения, добавления, удаления и обновления единицы выполнения посредством модуля управления и планирования единицы выполнения клиента DRM.

6. Способ управления цифровыми правами (DRM) мультимедиа-содержимого, осуществляемый на серверной стороне DRM, причем способ предусматривает:

стадия 1: прием серверной стороной DRM запроса авторизации DRM, отправленного клиентом DRM, при этом запрос авторизации DRM содержит уникальный идентификатор мультимедиа-содержимого и базовую информацию клиента DRM;

стадия 2: получение серверной стороной DRM алгоритма шифрования содержимого и ключа шифрования содержимого, применяемых для мультимедиа-содержимого, и полномочий DRM клиента DRM для мультимедиа-содержимого в соответствии с запросом авторизации DRM посредством запроса;

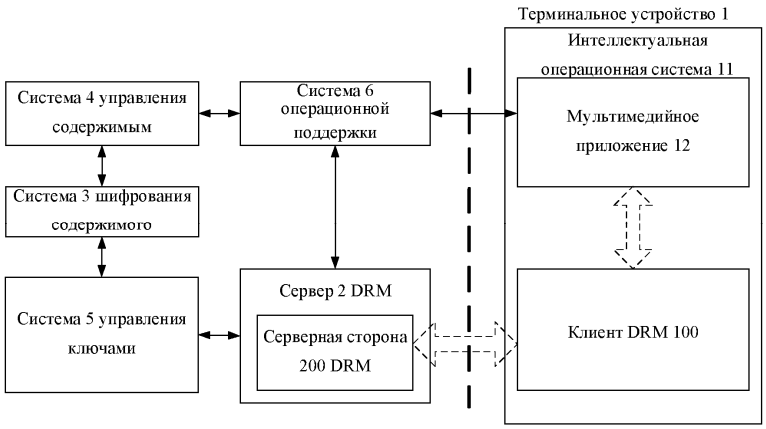
стадия 3: генерирование серверной стороной DRM единицы выполнения авторизации содержимого в соответствии с идентификатором мультимедиа-содержимого, алгоритмом шифрования содержимого и ключом шифрования содержимого, применяемых для мультимедиа-содержимого, базовой информацией клиента DRM и полномочиями DRM клиента DRM для мультимедиа-содержимого, при этом единица выполнения авторизации содержимого выполнена с возможностью выполнения в выполняемой среде клиента DRM таким образом, чтобы проверять, соответствует ли выполняемая среда терминала терминального устройства, где расположен клиент DRM, полномочиям DRM клиента DRM для мультимедиа-содержимого, и в случае соответствия расшифровывать мультимедиа-содержимое в соответствии с алгоритмом шифрования содержимого и ключом шифрования содержимого;

стадия 4: выдача серверной стороной DRM сгенерированной единицы выполнения авторизации содержимого клиенту DRM,

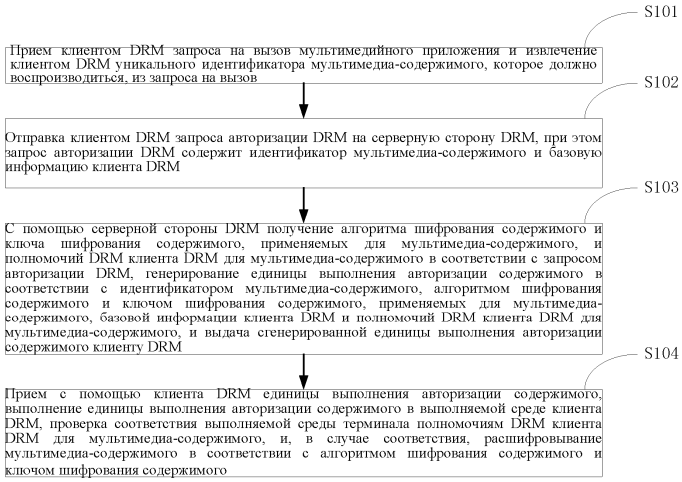
причем клиент DRM включает ядро единицы выполнения и модуль управления и планирования единицы выполнения, ядро единицы выполнения выполнено с возможностью выполнения единицы выполнения, а клиент DRM планирует и управляет единицами выполнения посредством модуля управления и планирования единицы выполнения, включая внесение в ядро единицы выполнения плана касательно единицы выполнения для выполнения, а единицы выполнения включают единицу выполнения авторизации содержимого.

7. Способ по п.6, дополнительно включающий стадию подписания единицы выполнения авторизации содержимого до того, как модуль выдачи единицы выполнения выдаст единицу выполнения авторизации содержимого, посредством модуля подписи единицы выполнения серверной стороны DRM.

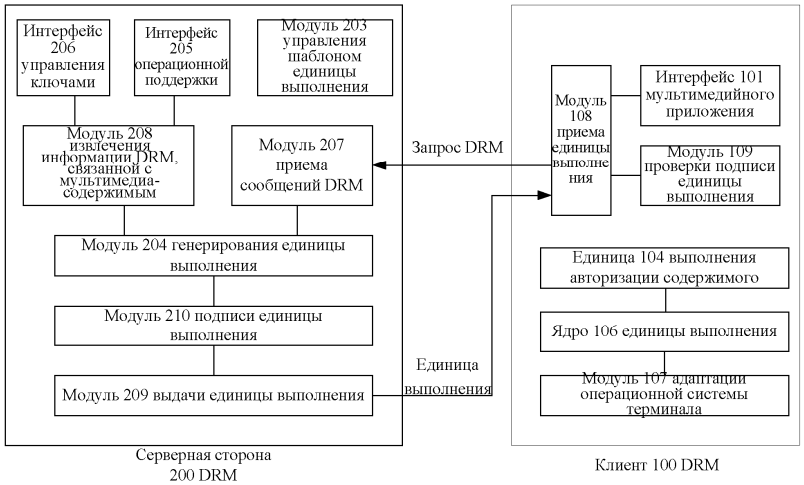
8. Способ по любому из пп.8 или 9, дополнительно включающий стадию управления шаблоном единицы выполнения авторизации содержимого, включая добавление, обновление и удаление шаблона единицы выполнения авторизации содержимого посредством модуля управления шаблоном единицы выполнения серверной стороны DRM.



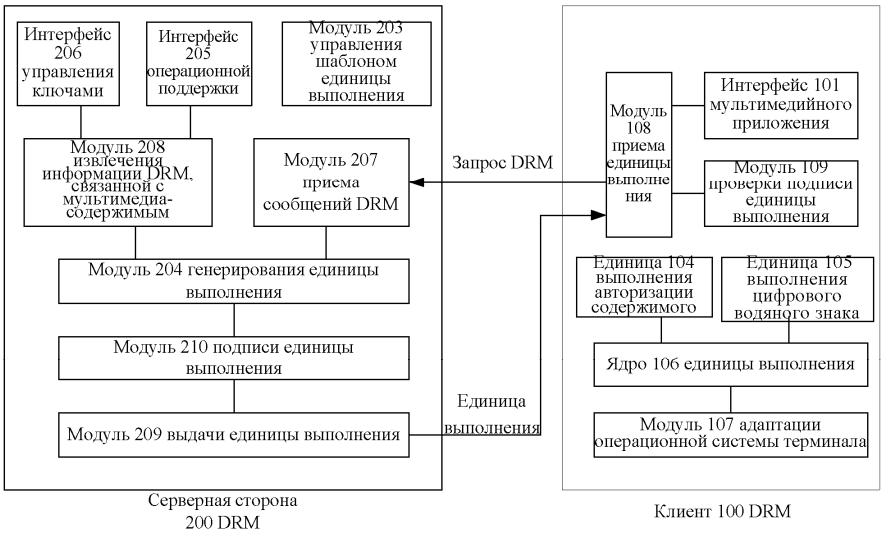
Фиг. 1



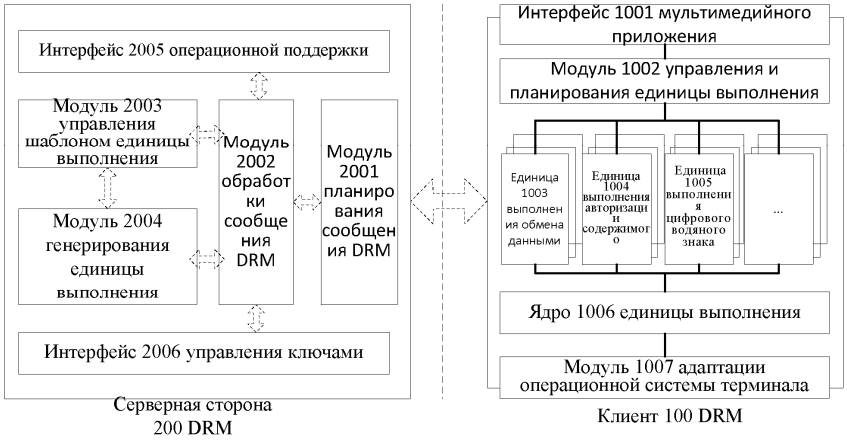
Фиг. 2



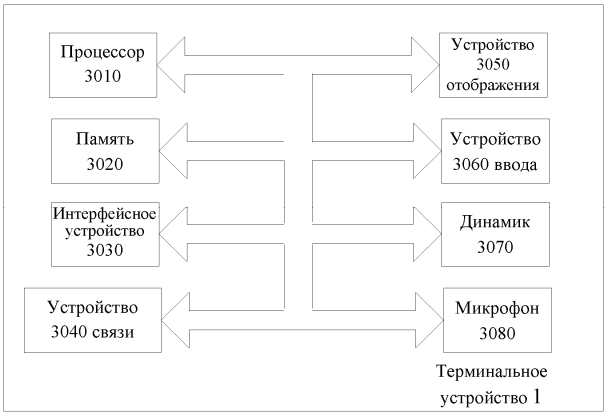
Фиг. 3



Фиг. 4


Интерфейс 2005 операционной поддержки
Модуль 2003 управления шаблоном единицы выполнения
Модуль 2004 генерирования единицы выполнения
Модуль 2002 обработки сообщения DRM
Модуль 2001 планирования сообщения DRM
Интерфейс 2006 управления ключами
Серверная сторона 200 DRM
Интерфейс 1001 мультимедийного приложения
Модуль 1002 управления и планирования единицы выполнения
Единица 1003 выполнения обмена данными
Единица 1004 выполнения авторизации и содержимого
Единица 1005 выполнения цифрового водяного знака
...
Ядро 1006 единицы выполнения
Модуль 1007 адаптации операционной системы терминала
Клиент 100 DRM

Фиг. 5


Процессор 3010
Память 3020
Интерфейсное устройство 3030
Устройство 3040 связи
Устройство 3050 отображения
Устройство 3060 ввода
Динамик 3070
Микрофон 3080
Терминальное устройство 1

Фиг. 6