РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(19) **RU** (11) **2 394 389** (13) **C2**

(51) МПК
H04N 5/917 (2006.01)
H04N 7/24 (2006.01)
G11B 20/10 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21), (22) Заявка: **2008105548/09, 12.07.2006**

(24) Дата начала отсчета срока действия патента:
12.07.2006

(30) Конвенционный приоритет:
14.07.2005 US 11/182,088

(43) Дата публикации заявки: **20.08.2009**

(45) Опубликовано: **10.07.2010** Бюл. № **19**

(56) Список документов, цитированных в отчете о поиске: **EP 1379084 A1, 07.01.2004. US 2003188182 A1, 02.10.2003. WO 03107665 A1, 24.12.2003. EP1122728 A1, 08.08.2001. US 2002006165 A1, 17.01.2002. WO 2005036876 A1, 21.04.2005. RU 2003113331 A, 10.10.2004. KIM G., SHIN D., Intellectual Property Management on MPEG-4 Video for Hand-Held Device and Mobile Video Streaming Service, IEEE Transactions on Consumer Electronics, vol.51, issue 1, February 2005.**

(85) Дата перевода заявки PCT на национальную фазу: **14.02.2008**

(86) Заявка PCT:
US 2006/027461 (12.07.2006)

(87) Публикация PCT:
WO 2007/011766 (25.01.2007)

Адрес для переписки:
129090, Москва, ул. Б.Спасская, 25, стр.3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. Ю.Д.Кузнецову, рег.№ 595

(72) Автор(ы):
УИНГЕРТ Кристофер Р. (US),
АГГАРВАЛ Пуджа (US)

(73) Патентообладатель(и):
КВЭЛКОММ ИНКОРПОРЕЙТЕД (US)

RU 2394389 C2

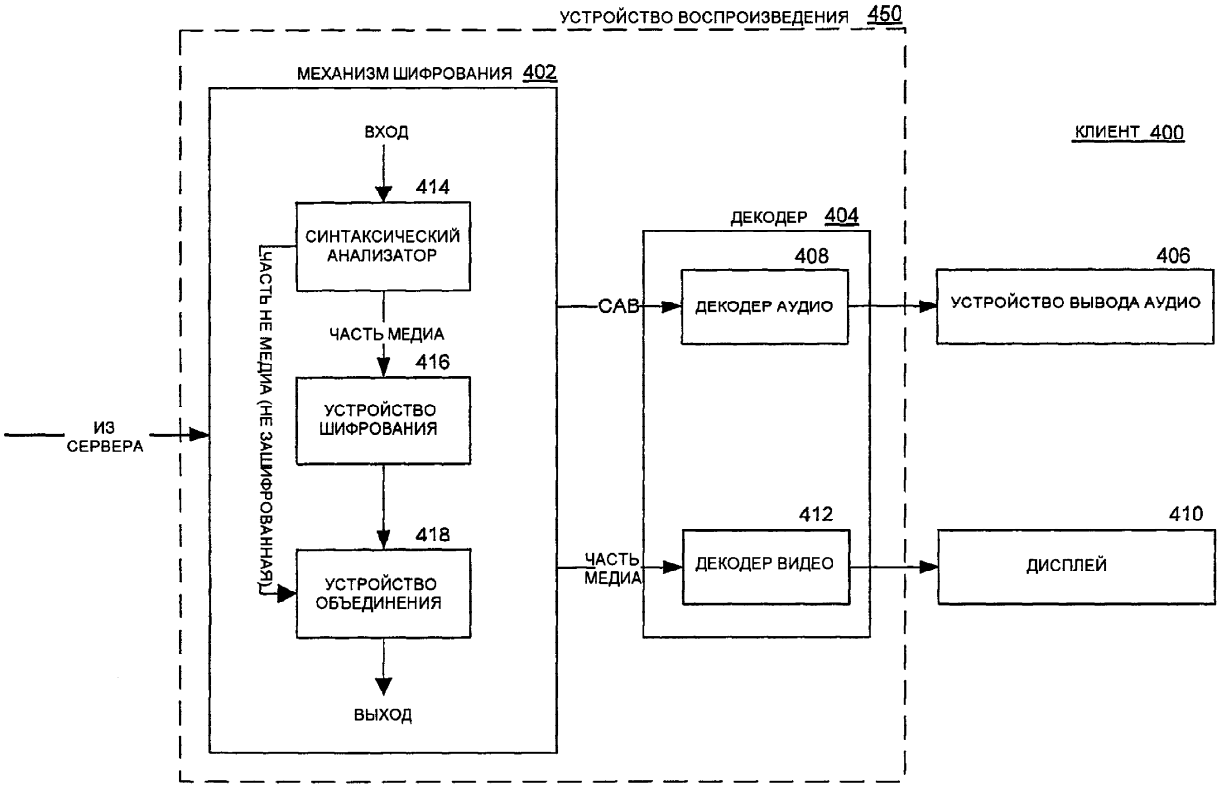
RU 2394389 C2

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ ШИФРОВАНИЯ/ДЕШИФРОВАНИЯ КОНТЕНТА МУЛЬТИМЕДИА ДЛЯ ОБЕСПЕЧЕНИЯ ВОЗМОЖНОСТИ ПРОИЗВОЛЬНОГО ДОСТУПА

(57) Реферат:

Изобретение относится к шифрованию и дешифрованию файлов мультимедиа. Техническим результатом является создание способа и устройства, предназначенных для шифрования только данных видео транспортного потока кодека и оставления нетронутым метаконтента. Таким образом, любая ошибка, байтовое расширение или сжатие данных будут минимизированы таким

образом, чтобы затрагивать небольшую часть воспроизведения мультимедиа. Предложен способ шифрования файла мультимедиа, включающий в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа, шифруют часть данных медиа и объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа. Также раскрыт способ для воспроизведения файла мультимедиа, включающий в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных, используют незашифрованную часть метаданных, чтобы определить местонахождение позиции, представляющей интерес, в файле медиа, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, и дешифруют связанную зашифрованную часть данных медиа. Также в настоящей заявке раскрыто устройство для выполнения упомянутых способов. 8 н. и 7 з.п. ф-лы, 6 ил.



Фиг. 4

RU 2394389 C2

RU 2394389 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(19) **RU** (11) **2 394 389** (13) **C2**

(51) Int. Cl.
H04N 5/917 (2006.01)
H04N 7/24 (2006.01)
G11B 20/10 (2006.01)

(12) ABSTRACT OF INVENTION

(21), (22) Application: **2008105548/09, 12.07.2006**

(24) Effective date for property rights:
12.07.2006

(30) Priority:
14.07.2005 US 11/182,088

(43) Application published: **20.08.2009**

(45) Date of publication: **10.07.2010 Bull. 19**

(85) Commencement of national phase: **14.02.2008**

(86) PCT application:
US 2006/027461 (12.07.2006)

(87) PCT publication:
WO 2007/011766 (25.01.2007)

Mail address:
129090, Moskva, ul. B.Spasskaja, 25, str.3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. Ju.D.Kuznetsovu, reg.№ 595

(72) Inventor(s):
UINGERT Kristofer R. (US),
AGGARVAL Pudzha (US)

(73) Proprietor(s):
KVEhLKOMM INKORPOREJTED (US)

RU 2394389 C2

RU 2394389 C2

(54) METHOD AND DEVICE FOR ENCRYPTING/DECRYPTING MULTIMEDIA CONTENT FOR ENABLING RANDOM ACCESS

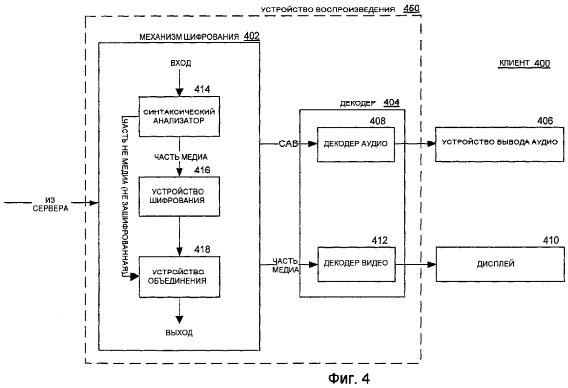
(57) Abstract:

FIELD: information technology.

SUBSTANCE: any error, byte extension or data compression will be minimised so as to affect a small multimedia playback part. A method for encrypting a multimedia file is disclosed, which involves steps on which syntax analysis of the multimedia file is carried out in order to identify part of the media data which is then encrypted and combined with an unencrypted part of non-media data. A method of playing back a multimedia file is also disclosed, which includes steps on which syntax analysis of the multimedia file is carried out in order to identify the unencrypted part of metadata which is then used to determine the position of interest in the media file, where the said position of interest has a related encrypted part of media data which is then decrypted. Disclosed also is a device for implementing the said methods.

EFFECT: design of a method and a device for encrypting only video data of the codec traffic stream, leaving meta-content untouched.

15 cl, 6 dwg



Фиг. 4

УРОВЕНЬ ТЕХНИКИ

Область техники, к которой относится изобретение

Варианты осуществления изобретения относятся в целом к шифрованию и дешифрованию файлов мультимедиа и, более конкретно, к способу и устройству, предназначенным для шифрования/дешифрования контента мультимедиа, чтобы дать возможность произвольного доступа.

Уровень техники

Так как развернуты 3G и другие сотовые сети, появляются новые службы, основанные на пакетных данных IP. Одна из наиболее перспективных областей служб, которую пытаются использовать операторы, включает в себя распространение видеоконтента в массовый рынок. Высококачественное видео является наиболее интенсивным с точки зрения данных типом контента. В то же время опыт потребителя с современными вариантами домашнего просмотра преподносит операторам и провайдерам контента целевые рынки, которые содержат устоявшиеся идеи о том, какой должен быть опыт пользователя. Сочетание ожиданий потребителей и мобильности представляет собой основные проблемы для операторов сетей и провайдеров контента. Итак, привлекательные модели деловой деятельности, управление и администрирование сетей, управление доступом, функциональные возможности устройств и убедительный пользовательский опыт комбинируются, предоставляя комплекс взаимозависимых проблем, которые не полностью решены в беспроводной индустрии.

Одной проблемой, которая возникла, является потребность обеспечивать защиту контента, который должен быть распространен. Например, распространяемый контент должен быть защищен от несанкционированного копирования. Кроме того, провайдеры контента также желают управлять, либо непосредственно, либо косвенно, распространением контента. Таким образом, провайдеры контента обычно требуют, чтобы любая система распространения контента, используемая провайдером службы, имела возможность обеспечивать управление цифровыми правами (DRM), которое относится к любому из нескольких технических устройств, которые обеспечивают контроль относительно того, как распространяемый материал может быть использован в любом электронном устройстве, установленном с такими оценками. Важным основным компонентом для всех систем распределения контента, чтобы поддерживать DRM таким образом, чтобы защищать права на интеллектуальную собственность провайдеров контента, является функциональная возможность шифрования/дешифрования медиа во время передачи/приема. Кроме того, часто требованием является сохранять медиа в зашифрованном виде, либо в серверах в центре распространения, либо в устройстве воспроизведения. Кроме того, шифрование часто требует поддерживать “трюковые” функциональные возможности, такие как возможность просматривать контент во время быстрой перемотки вперед и перемотки назад. Желательно, чтобы решение шифрования медиа обеспечивало шифрование с минимальными изменениями в интерфейсе кодирования видео.

Сущность изобретения

Варианты осуществления, описанные в настоящей заявке, предоставляют способы и устройства, предназначенные для шифрования только данных видео транспортного потока кодека и оставления нетронутым метаконтента. Таким образом, любая ошибка, байтовое расширение или сжатие данных будут минимизированы таким образом, чтобы затрагивать небольшую часть воспроизведения мультимедиа.

В одном варианте осуществления в настоящей заявке описан способ,

предназначенный для шифрования файла мультимедиа, причем способ включает в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа, шифруют часть данных медиа и объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа. В настоящей заявке также предоставлен способ, предназначенный для воспроизведения файла мультимедиа, предназначенный для выполнения синтаксического анализа файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных, использования незашифрованной части метаданных, чтобы определить местонахождение позиции, представляющей интерес, в файле медиа, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, и дешифрования связанной зашифрованной части данных медиа.

В другом варианте осуществления в настоящей заявке описан процессор, сконфигурированный с возможностью осуществления способа, предназначенного для шифрования файла мультимедиа, причем способ включает в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа, шифруют часть данных медиа и объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа. В этом другом варианте осуществления в настоящей заявке также предоставлен процессор, сконфигурированный с возможностью осуществления способа, предназначенного для воспроизведения файла мультимедиа, причем способ включает в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных, используют незашифрованную часть метаданных, чтобы определить местонахождение позиции, представляющей интерес, в файле медиа, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, и дешифруют связанную зашифрованную часть данных медиа.

В еще одном варианте осуществления в настоящей заявке описан машиночитаемый носитель, имеющий запомненные в нем инструкции, причем запомненные инструкции при выполнении с помощью процессора заставляют процессор выполнять способ, предназначенный для шифрования файла мультимедиа, причем способ включает в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа, шифруют часть данных медиа и объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа. В этом другом варианте осуществления в настоящей заявке также предоставлен машиночитаемый носитель, имеющий запомненные в нем инструкции причем запомненные инструкции, при выполнении с помощью процессора заставляют процессор выполнять способ, предназначенный для воспроизведения файла мультимедиа, причем способ включает в себя этапы, на которых выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных, используют незашифрованную часть метаданных, чтобы определить местонахождение позиции, представляющей интерес, в файле медиа, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, и дешифруют связанную зашифрованную часть данных медиа.

Еще в одном варианте осуществления в настоящей заявке описано устройство, предназначенное для шифрования файла мультимедиа, причем устройство включает в себя средство, предназначенное для выполнения синтаксического анализа файла мультимедиа, чтобы идентифицировать часть данных медиа, средство,

предназначенное для шифрования части данных медиа, и средство, предназначенное для объединения зашифрованной части данных медиа с незашифрованной частью данных не медиа. В этом другом варианте осуществления в настоящей заявке также описано устройство, предназначенное для воспроизведения файла мультимедиа, имеющее средство, предназначенное для выполнения синтаксического анализа файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных, средство, предназначенное для использования незашифрованной части метаданных, чтобы определить местонахождение позиции, представляющей интерес, в файле медиа, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, и средство, предназначенное для дешифрования связанной зашифрованной части данных медиа.

Другие задачи, признаки и преимущества станут более понятными специалистам в данной области техники из следующего подробного описания. Однако следует понимать, что подробное описание и специфические примеры, несмотря на то, что показывают примерные варианты осуществления, даны в качестве иллюстрации, а не ограничения. Многие изменения и модификации в рамках объема следующего описания могут быть сделаны, не выходя за рамки сущности описания, и описание следует понимать, как включающее в себя все такие модификации.

Краткое описание чертежей

Изобретение может быть более легко понято с помощью ссылки на сопровождающие чертежи, на которых:

фиг.1 - фигура, иллюстрирующая организацию примерного битового потока видео, как определено с помощью стандартного кодека;

фиг.2 - фигура, иллюстрирующая организацию выборок для выборок видео и аудио в порции данных и смещения порций данных;

фиг.3 - блок-схема сервера с механизмом шифрования, сконфигурированным с возможностью шифрования только части медиа контента мультимедиа;

фиг.4 - блок-схема клиента с устройством воспроизведения, чтобы дешифровать и воспроизводить зашифрованную часть медиа контента мультимедиа;

фиг.5 - блок-схема последовательности этапов работы механизма шифрования; и

фиг.6 - блок-схема пункта доступа и терминала доступа, используемых для осуществления признаков, описанных в настоящей заявке.

Одинаковые номера относятся к одинаковым частям по всем нескольким видам чертежей.

Подробное описание предпочтительных вариантов осуществления

Варианты осуществления, предоставленные в настоящей заявке, предоставляют способ, предназначенный для шифрования только части “контента” данных любого транспортного потока кодека и оставления нетронутым метаконтента, который используют, чтобы определить местонахождение и воспроизвести контент. Например, в одном варианте осуществления шифруют только часть контента видео. В результате влияния любой ошибки или расширения/сжатия данных должны быть минимизированы и, таким образом, затрагивают небольшую часть воспроизведения мультимедиа.

Следующее описание предполагает, что кодек, используемый для того, чтобы сохранять контент мультимедиа, согласуется со стандартом MPEG-4, как опубликовано группой экспертов в области движущихся изображений (MPEG), рабочей группой Международной организации стандартизации/Международной электротехнической комиссии, Объединенного технического комитета 1 (ISO/IEC

JTC1). Стандарты ISO/IEC обозначены с помощью MPEG-x (например, MPEG-1, MPEG-2 и MPEG-4), а стандарт MPEG-4 описан в ISO/IEC 14496-2.

Файл MPEG-4 состоит из иерархических элементарных единиц, включающих в себя элементарные единицы метаданных и данных медиа. Каждая элементарная единица сама может быть составлена из других элементарных единиц. Элементарные единицы метаданных и данных медиа могут присутствовать где угодно в файле. Обычно элементарная единица (**moov**) является необязательной и может быть расположена либо до, либо после элементарных единиц данных медиа в файле. Метаданные обычно составляют менее чем 5-10% от файла MPEG-4.

Каждая элементарная единица сама имеет поле типа и размера, назначенное ей, из которого может быть сгенерирована карта контента файла. Это дает возможность синтаксическому анализатору устройства воспроизведения мультимедиа быстро переходить от одной элементарной единицы к другой. Каждый элементарный поток, такой как поток аудио или поток видео, будет иметь свою собственную элементарную единицу **mdat** (данные медиа). В элементарной единице **mdat** данные медиа организованы в виде порций данных, которые являются набором связанных выборок. Например, порция данных видео может включать в себя первые три кадра видео последовательности видео (например, кадры 1, 2 и 3), в то время как порция данных аудио могла бы иметь в ней одну или более выборок аудио. Эти порции данных медиа разбросаны по всему файлу.

Элементарная единица метаданных содержит информацию о среде в файле, о кадрах и их смещениях. Конкретно, в элементарной единице **moov** присутствует элементарная единица **stbl** или элементарная единица таблицы выборки. Эта элементарная единица **stbl** дополнительно состоит из следующих элементарных единиц таблицы:

stts: преобразует время в номера выборок

stsz: задает размер выборки

stsc: преобразует выборки в порции данных (по существу, указывает, какая выборка имеет место в какой порции данных)

stco: предоставляет смещение порции данных в файле

stsd: таблица описания выборок, которая содержит информацию о конфигурации (заголовки VOL и т.д.).

Вместе эти элементарные единицы предоставляют важные метаданные, необходимые для синтаксического анализа, в соответствующий кадр или выборку аудио, чтобы визуализировать ее для воспроизведения, как дополнительно описано ниже.

Многие устройства воспроизведения мультимедиа являются основанными на файлах, таким образом, что они берут в качестве входных данных имя файла или буфер, содержащий файл мультимедиа. Устройство воспроизведения выполняет сканирование метаданных файла, чтобы загрузить внутреннюю таблицу с информацией о смещениях кадров и хронирования. Необработанные кадры загружают в кодек (например, кодек MPEG-4) для декодирования, а затем визуализируют на дисплее с помощью устройства воспроизведения. Внутреннюю таблицу используют, чтобы выполнить такие функции, как “быстрые” установки в соответствующую позицию в файле во время быстрой перемотки вперед или перемотки назад, или воспроизведение с “произвольным доступом” из любой точки в файле. Такие функциональные возможности совместно упоминают как функциональные возможности “трюкового воспроизведения”.

Чтобы хранить внутренние таблицы в сжатом виде, используют множество способов. Один способ, который используют, чтобы сжимать информацию о местонахождении и размере, полагается на наблюдение, что несколько выборок из одной и той же дорожки часто сохраняют как смежные друг другу, даже когда данные из разных дорожек перемежуют. Этот отрезок смежных выборок из конкретной дорожки называют порцией данных. Таблица соответствия дорожки порции данных в обязательной элементарной единице 'stsc' предоставляет преобразование из номера выборки в индексы порций данных. (Абсолютную) позицию каждой порции данных записывают в обязательной элементарной единице 'stco' как смещение порции данных (с использованием 32 или 64 бит), которое измеряют от начала файла, в котором расположена порция данных. Длину в байтах каждой выборки также записывают в таблице размера выборки в обязательной элементарной единице 'stsz'. Следовательно, с помощью использования:

1. указателя данных из дорожки,
2. преобразования выборки в порцию данных,
3. смещения порции данных, и
4. размеров предшествующих выборок в одной и то же порции данных

можно найти:

1. файл данных, содержащий выборку, который может быть файлом, указанным с помощью URL из самого файла MP4,
2. порцию данных (и ее смещение) в этом файле,
3. смещение выборки в порции данных (из размеров предшествующих выборок в одной и той же порции данных), и
4. размер самой выборки.

Фиг.2 иллюстрирует простой пример, связанный с этим процессом. Следует заметить, что размеры как кадра видео, так и кадра аудио, являются также известными, границы любых выборок видео или аудио могут быть без труда вычислены как абсолютные смещения. В таком устройстве воспроизведения предварительно созданная структура таблицы не дает возможность загрузки зашифрованных файлов в устройство воспроизведения. Входные данные устройства воспроизведения являются в виде либо имени файла (char*), либо буфера, что предполагает, что весь файл расположен в незашифрованном формате в буфере. Никакой из этих интерфейсов не дает возможности устройству воспроизведения расшифровывать файл “потоковым” способом (т.е. выполнение дешифрования во время воспроизведения файла).

В одном варианте осуществления потоковая функциональная возможность может быть добавлена, если систему шифрования/дешифрования модифицируют таким образом, что шифрование происходит в кадре или на уровне секции с оставлением метаданных в исходном состоянии, чтобы поддерживать трюковое воспроизведение. Этот способ “интеллектуального шифрования” дает возможность системе шифрования (например, серверу) быть осведомленным о формате медиа, во время шифрования фактического контента и оставления важных метаданных и данных заголовка в исходном состоянии. Подобным образом, в системе дешифрования (например, клиенте) метаданные могут быть использованы, чтобы выполнять функции, такие как трюковое воспроизведение, без дополнительной обработки, так как они являются незашифрованными, и только часть контента потока или файла должна быть дешифрована.

Следует заметить, что, несмотря на то, что каждая часть схемы шифрования может

быть конкретно описана в настоящей заявке в понятиях части медиа, отделенной от части не медиа (например, метаданных), а затем зашифрованной, в одном варианте осуществления система шифрования будет выполнять синтаксический анализ файла/потока медиа и во время синтаксического анализа файла/потока медиа шифровать только части данных медиа и оставлять метаданные как они есть. Таким образом, в одном варианте осуществления часть медиа не должна быть отделена от метаданных, зашифрована, а затем возвращена обратно вместе (т.е. мультиплексирована) с метаданными. В другом варианте осуществления часть медиа может быть отделена для обработки и требует мультиплексирования. В любом сценарии к системам и процессам, внешним к системе шифрования, оба варианта осуществления также применяются в части схемы дешифрования.

Фиг.3 иллюстрирует сервер 300 с механизмом 302 шифрования, который включает в себя синтаксический анализатор 308, который выполняет синтаксический анализ входящих данных из источника 332 мультимедиа, которые могут быть из потока или файла, в части медиа и не медиа. Процессор 306 шифрования, в то время как синтаксический анализатор 308 выполняет синтаксический анализ входящих данных, затем шифрует только части медиа с использованием информации из сервера 322 DRM.

Устройство 304 объединения будет объединять часть не медиа (которая не зашифрована) и зашифрованную часть медиа и посылать ее в постпроцессор 352 для передачи клиенту 400, как изображено на фиг.4.

Интеллектуальное шифрование потребовало бы механизм 302 шифрования, который учитывает разные форматы медиа, поддерживаемые системой, таким образом, что он шифровал бы только данные кадра, оставляя заголовки в исходном состоянии. Например, в случае MPEG-4, как проиллюстрировано на фиг.1, система шифровала бы только данные VOP и оставляла бы заголовки GOV и VOP в исходном состоянии. Кроме того, допуская, что битовый поток видео является стандартным файлом MP-4, когда элементарная единица метаданных **stbl** является обязательной, механизм шифрования не должен был бы выполнять синтаксический анализ для кодов кадра или начала выборки аудио, чтобы добраться к данным медиа. Вместо этого механизм шифрования использовал бы информацию в элементарной единице метаданных **stbl**, чтобы выполнить синтаксический разбор в соответствующей позиции в файле, чтобы добраться к данным кадра или выборки аудио.

Фиг.4 иллюстрирует клиента 400, который принимает файл мультимедиа из сервера 300 и дешифрует соответствующие части принятого файла для визуализации и воспроизведения. Устройство 450 воспроизведения могло бы создать внутреннюю таблицу без какого-либо дешифрования, так как вся информация заголовка файла находится в исходном состоянии. Устройство 450 воспроизведения включало бы в себя механизм 402 дешифрования, и синтаксический анализатор 414 в механизме 402 дешифрования передавал бы часть файла, которая зашифрована, в устройство 416 дешифрования вместе с ключом для дешифрования до посылки кадров в кодек MP-4. Конкретно, синтаксический анализатор 414 извлекает данные для зашифрованных кадров и посылает их в устройство 416 дешифрования. Часть не медиа, которая не была зашифрована с помощью сервера 300, была бы непосредственно послана в устройство 418 объединения для объединения с зашифрованной частью медиа. Декодер 404, который включает в себя декодер 408 аудио и декодер 412 видео, декодировал бы закодированный битовый поток аудио (CAB) и закодированный битовый поток видео (CVB) для визуализации в устройстве 406 вывода аудио и дисплее 410, соответственно. Следует заметить, что устройство 450 воспроизведения

может иметь больше компонентов, чем проиллюстрировано на фиг.4.

В описанном выше варианте осуществления файл выглядел бы как обычный файл MPEG-4 для устройства воспроизведения, так как заголовки являются незашифрованными. Создание внутренней таблицы не потребовало бы, чтобы происходило какое-либо описание, таким образом, описание будет происходить только, когда кадры загружены в кодек. Конечно, оба механизма шифрования/дешифрования должны быть осведомлены о файловом формате, чтобы распознать заголовок. Таким образом, были бы изменения, необходимые для каждого дополнительного формата медиа, который должна поддерживать система. Кроме того, будет дополнительная нагрузка обработки на механизм шифрования, чтобы дать возможность шифрования на уровне кадра, синтаксического разбора элементарной единицы **stbl**, поиска данных медиа и т.д.

Фиг.5 иллюстрирует блок-схему последовательности этапов примерного варианта осуществления работы процесса 500 шифрования/дешифрования, в которой в блоке 502 синтаксический анализатор 308 механизма 302 шифрования определяет, принадлежат ли данные, принятые из файла или потока, части медиа или части не медиа. Если принадлежат, тогда работа продолжается с помощью блока 504, в котором устройство 306 шифрования шифрует часть медиа. Иначе работа продолжается с помощью блока 508, в котором не шифруют часть данных не медиа (т.е. оставляют в исходном состоянии). В блоке 506 части медиа и не медиа объединяют и считывают в местонахождение сохранения файла (такое как запоминающее устройство в сервере 300) или выводят в виде потока клиенту 400. Если весь файл или поток не обработан, тогда работа возвращается в блок 502. Иначе данные передают клиенту 400.

Когда данные переданы клиенту 400 либо в файле, либо как часть потока, во время воспроизведения клиент 400 может считать часть метаданных в блоке 512, а в блоке 514 определяет, найдено ли местонахождение воспроизведения. Если найдено, тогда работа продолжается с помощью блока 516, в котором считывают и дешифруют часть медиа. Дешифрованную часть затем предоставляют в декодер 404 для воспроизведения, как описано выше.

Фиг.6 изображает блок-схему пункта 604x доступа и терминала 602x доступа, которые могут быть использованы, чтобы передавать и принимать, соответственно, данные, зашифрованные с использованием способов и устройств, описанных в настоящей заявке. Как описано в настоящей заявке, “терминал доступа” относится к устройству, обеспечивающему возможность речевой связи и/или связи данных пользователю. Терминал доступа может быть соединен с вычислительным устройством, таким как переносной портативный компьютер или настольный компьютер, или он может быть самостоятельным устройством, таким как персональный цифровой ассистент. Терминал доступа также может быть назван абонентским устройством, подвижной станцией, подвижным устройством, дистанционным устройством, дистанционным терминалом, пользовательским терминалом, пользовательским агентом или пользовательской аппаратурой. Терминал доступа может быть абонентской станцией, беспроводным устройством, сотовым телефоном, телефоном PCS, беспроводным телефоном, телефоном протокола инициализации сеанса (SIP), станцией беспроводной местной линии (WLL), персональным цифровым ассистентом (PDA), ручным устройством, имеющим функциональную возможность беспроводного соединения, или другим обрабатывающим устройством, соединенным с беспроводным модемом. Кроме того,

“пункт доступа”, как используемый в настоящем описании, относится к устройству в сети доступа, которое взаимодействует через эфирный интерфейс посредством одного или более секторов с терминалами доступа. Пункт доступа действует в качестве маршрутизатора между терминалом доступа и остальной сетью доступа, которая может включать в себя сеть IP, с помощью преобразования принятых кадров эфирного интерфейса в пакеты IP. Пункт доступа также координирует управление атрибутами для эфирного интерфейса.

Для обратной линии связи в терминале доступа 602x процессор 614 передачи (TX) данных принимает данные трафика из буфера 612 данных, обрабатывает (т.е. кодирует, перемежует и преобразует) символы каждого пакета данных на основании выбранной схемы кодирования и модуляции и предоставляет символы данных. Символ данных является символом модуляции для данных, а пилот-символ является символом модуляции для пилот-сигнала (который известен априори). Модулятор 616 принимает символы данных, пилот-символы и, возможно, сигнализацию для обратной линии связи, выполняет (например, OFDM) модуляцию и/или другую обработку, как определено системой, и предоставляет поток выходных элементарных посылок. Устройство 618 передатчика (TMTR) обрабатывает (например, преобразует в аналоговый вид, фильтрует, усиливает и преобразует с повышением частоты) поток выходных элементарных посылок и генерирует модулированный сигнал, который передают из антенны 620.

В пункте доступа 604x модулированный сигнал, переданный с помощью терминала 602x доступа и других терминалов, находящихся на связи с пунктом 604x доступа, принимают с помощью антенны 652. Устройство 654 приемника (RCVR) обрабатывает (например, предварительно формирует и преобразует в цифровой вид) принятый сигнал из антенны 652 и предоставляет принятые выборки. Демодулятор 656 (Demod) обрабатывает (например, демодулирует и детектирует) принятые выборки и предоставляет детектированные символы данных, которые являются оценкой шума символов данных, переданных с помощью терминалов в пункт 604x доступа. Процессор 658 данных приема (RX) обрабатывает (восстанавливает символы, удаляет перемежение и декодирует) детектированные символы данных для каждого терминала и предоставляет декодированные данные для этого терминала.

Для прямой линии связи в пункте 604x доступа данные трафика обрабатывают с помощью процессора 660 данных TX, чтобы сгенерировать символы данных. Модулятор 662 принимает символы данных, пилот-символы и сигнализацию для прямой линии связи, выполняет (например, OFDM) модуляцию и/или другую подходящую обработку и предоставляет выходной поток элементарных посылок, который дополнительно предварительно формируют с помощью устройства 664 передатчика, и передают из антенны 652. Сигнализация прямой линии связи может включать в себя команды управления мощностью, генерируемые с помощью контроллера 670 для всех терминалов, передающих по обратной линии связи в пункт доступа 604x. В терминале 602x доступа модулированный сигнал, переданный с помощью пункта 604x доступа, принимают с помощью антенны 620, предварительно формируют и преобразуют в цифровой вид с помощью устройства 622 приемника и обрабатывают с помощью демодулятора 624, чтобы получить детектированные символы данных. Процессор 1026 данных RX обрабатывает детектированные символы данных и предоставляет декодированные данные для терминала и сигнализацию прямой линии связи. Контроллер 630 принимает команды управления

мощностью и управляет передачей данных, и передает мощность по обратной линии связи в пункт 604x доступа. Контроллеры 630 и 670 управляют работой терминала 602x доступа и пункта 604x доступа, соответственно. Устройства 632 и 672 памяти сохраняют коды программ и данные, используемые контроллерами 630 и 670, соответственно.

Раскрытые варианты осуществления могут быть применены к любой из комбинаций следующих технологий: системы множественного доступа с кодовым разделением (CDMA), система многоканального CDMA (MC- CDMA), система широкополосного CDMA (W- CDMA), система высокоскоростного пакетного доступа прямой линии связи (HSDPA), системы множественного доступа с разделением времени (TDMA), системы множественного доступа с частотным разделением (FDMA) и системы множественного доступа с ортогональным частотным уплотнением (OFDMA).

Этапы способа или алгоритма, описанного в связи с вариантами осуществления, раскрытыми в настоящей заявке, могут быть осуществлены непосредственно в аппаратном обеспечении, в модуле программного обеспечения, выполняемом процессором, или в комбинации того и другого. Модуль программного обеспечения может находиться в памяти RAM, флэш-памяти, памяти ROM, памяти EPROM (электрически программируемое ПЗУ), памяти EEPROM (электрически стираемое программируемое ПЗУ), в регистрах, на жестком диске, сменном диске, CD-ROM, или любом другом виде запоминающего носителя, известного в данной области техники. Примерный запоминающий носитель соединен с процессором таким образом, что процессор может считывать информацию из запоминающего носителя и записывать информацию на него. В качестве альтернативы запоминающий носитель может быть единым целым с процессором. Процессор и запоминающий носитель могут находиться в ASIC. ASIC может находиться в пользовательском терминале. В качестве альтернативы процессор и запоминающий носитель могут находиться в дискретных компонентах в пользовательском терминале.

Следует заметить, что способы, описанные в настоящей заявке, могут быть осуществлены в множестве аппаратного обеспечения, процессоров и систем, известных обычному специалисту в данной области техники. Например, общим требованием для клиента, чтобы работать, как описано в настоящей заявке, является то, что клиент имеет дисплей, чтобы отображать контент и информацию, процессор, чтобы управлять работой клиента, и память для сохранения данных и программ, связанных с работой клиента. В одном варианте осуществления клиент является сотовым телефоном. В другом варианте осуществления клиент является карманным компьютером, имеющим функциональные возможности связи. Еще в одном варианте осуществления клиент является персональным компьютером, имеющим функциональные возможности связи. Кроме того, аппаратное обеспечение, такое как приемник GPS, может быть встроенным, когда необходимо, в клиенте, чтобы осуществлять различные варианты осуществления, описанные в настоящей заявке.

Различные иллюстративные логические схемы, логические блоки, модули и схемы, описанные в связи с вариантами осуществления, раскрытыми в настоящей заявке, могут быть осуществлены или выполнены с помощью процессора общего назначения, процессора цифровых сигналов (DSP), специализированной интегральной схемы (ASIC), вентильной матрицы, программируемой в условиях эксплуатации (FPGA) или другого программируемого логического устройства, дискретной логической схемы или транзисторной логики, дискретных компонентов аппаратного обеспечения

или любой их комбинации, предназначенной для выполнения функций, описанных в настоящей заявке. Процессор общего назначения может быть микропроцессором, но в альтернативе процессор может быть любым традиционным процессором, контроллером, микроконтроллером или конечным автоматом. Процессор также может быть реализован как комбинация вычислительных устройств, например комбинация DSP и микропроцессора, множество микропроцессоров, один или более микропроцессоров совместно с ядром DSP или любая другая такая конфигурация.

Варианты осуществления, описанные выше, являются примерными вариантами осуществления. Специалисты в данной области техники теперь могут сделать многочисленные использования вышеописанных вариантов осуществления и отклонения от вышеописанных вариантов осуществления, не выходя за рамки изобретательных концепций, раскрытых в настоящей заявке. Различные модификации этих вариантов осуществления могут быть без труда понятны специалистам в данной области техники, а основные принципы, определенные в настоящей заявке, могут быть применены к другим вариантам осуществления, например, в службе мгновенных сообщений или любых обычных приложениях беспроводной передачи данных, не выходя за рамки сущности и объема новых аспектов, описанных в настоящей заявке. Следовательно, не предполагается, что рамки объема настоящего изобретения ограничены вариантами осуществления, изображенными в настоящей заявке, а должно соответствовать самым широким рамкам объема, согласующимся с принципами и новыми признаками, раскрытыми в настоящей заявке. Слово “примерный” использовано в настоящей заявке исключительно, чтобы означать ”служащий в качестве примера, образца или иллюстрации”. Вариант осуществления, описанный в настоящей заявке как ”примерный”, не обязательно должен быть истолкован как предпочтительный или преимущественный относительно других вариантов осуществления.

Формула изобретения

1. Способ для шифрования файла мультимедиа, содержащий этапы, на которых:

выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа посредством:

определения файлового формата файла мультимедиа; и

идентифицируют местоположение части данных медиафайла мультимедиа на основании определенного файлового формата, причем идентификация местоположения части данных медиа в файле мультимедиа, содержит:

преобразование выборки в порцию данных;

определение смещения выборки в порции данных; и

определение размеров предшествующих выборок в одной и той же порции данных, шифруют упомянутую часть данных медиа; и

объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа.

2. Способ по п.1, в котором часть данных медиа включает в себя множество видеокадров, и этап, на котором шифруют часть данных медиа, содержит шифрование части данных медиа на основе видеокадр за видеокадром.

3. Способ по п.1, в котором часть данных медиа включает в себя множество выборок аудио, и этап, на котором шифруют часть данных медиа, содержит шифрование части данных медиа на основе выборка аудио за выборкой аудио.

4. Способ для воспроизведения файла мультимедиа, содержащий этапы, на которых:

выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных посредством определения файлового формата файла мультимедиа; и

на основании определенного файлового формата идентифицируют незашифрованную часть не медиафайла мультимедиа используют незашифрованную часть метаданных, чтобы определить местонахождение позиции, представляющей интерес, в мультимедиа файле, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, причем определение местонахождения позиции, представляющей интерес, в файле медиа, содержит:

определение местонахождения выборки в файле медиа, посредством преобразования выборки в порцию данных; и

определения смещения выборки в порции данных; и дешифруют связанную зашифрованную часть данных медиа.

5. Процессор, сконфигурированный с возможностью осуществления способа для шифрования файла мультимедиа, причем способ содержит этапы, на которых:

выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа посредством определения файлового формата мультимедиа файла; и

идентифицируют местоположение части данных медиа файла мультимедиа на основании определенного файлового формата, причем идентификация местоположения части данных медиа в файле мультимедиа, содержит:

преобразование выборки в порцию данных; определение смещения выборки в порции данных; и

определение размеров предшествующих выборок в одной и той же порции данных, и шифруют часть данных медиа; и

объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа.

6. Процессор по п.5, в котором часть данных медиа включает в себя множество видеокадров, и этап, на котором шифруют часть данных медиа, содержит этап, на котором шифруют часть данных медиа на основе видеокадр за видеокадром.

7. Процессор по п.5, в котором часть данных медиа включает в себя множество выборок аудио, и этап, на котором шифруют часть данных медиа, содержит этап, на котором шифруют часть данных медиа на основе выборка аудио за выборкой аудио.

8. Процессор, сконфигурированный с возможностью осуществления способа для воспроизведения файла мультимедиа, причем способ включает в себя этапы, на которых:

выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных посредством определения файлового формата файла мультимедиа; и

на основании определенного файлового формата идентифицируют незашифрованную часть не медиа мультимедиа файла используют незашифрованную часть метаданных, чтобы определить местонахождение позиции, представляющей интерес, в мультимедиа файле, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, причем определение местонахождения позиции, представляющей интерес, в файле медиа, содержит:

определение местонахождения выборки в файле медиа, посредством преобразования выборки в порцию данных; и определения смещения выборки в порции данных; и

дешифруют связанную зашифрованную часть данных медиа.

9. Машиночитаемый носитель, имеющий сохраненные на нем инструкции, причем сохраненные инструкции при выполнении с помощью процессора заставляют процессор выполнять способ для шифрования файла мультимедиа, причем способ содержит этапы, на которых:

выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать часть данных медиа посредством определения файлового формата мультимедиа файла; и

идентифицируют местоположения части данных медиа файла мультимедиа на основании определенного файлового формата, причем идентификация местоположения части данных медиа в файле мультимедиа, содержит:

преобразование выборки в порцию данных; определение смещения выборки в порции данных; и

определение размеров предшествующих выборок в одной и той же порции данных, и шифруют часть данных медиа; и

объединяют зашифрованную часть данных медиа с незашифрованной частью данных не медиа.

10. Машиночитаемый носитель по п.9, в котором часть данных медиа включает в себя множество видеокадров, и этап, на котором шифруют часть данных медиа, содержит этап, на котором шифруют часть данных медиа на основе видеокадр за видеокадром.

11. Машиночитаемый носитель по п.9, в котором часть данных медиа включает в себя множество выборок аудио, и этап, на котором шифруют часть данных медиа, содержит этап, на котором шифруют часть данных медиа на основе выборка аудио за выборкой аудио.

12. Машиночитаемый носитель, имеющий сохраненные на нем инструкции, причем сохраненные инструкции при выполнении с помощью процессора заставляют процессор выполнять способ для воспроизведения файла мультимедиа, причем способ содержит этапы, на которых:

выполняют синтаксический анализ файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных посредством определения файлового формата мультимедиа файла; и

на основании определенного файлового формата идентифицируют незашифрованную часть не медиафайла мультимедиа используют незашифрованную часть метаданных, чтобы определить местонахождение позиции, представляющей интерес, в мультимедиа файле, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, причем определение местонахождения позиции, представляющей интерес, в файле медиа, содержит:

определение местонахождения выборки в файле медиа, посредством преобразования выборки в порцию данных; и

определения смещения выборки в порции данных; и дешифруют связанную зашифрованную часть данных медиа.

13. Устройство для шифрования файла мультимедиа, причем устройство содержит:

средство для выполнения синтаксического анализа файла мультимедиа, чтобы идентифицировать часть данных медиа содержащее:

средство для определения файлового формата файла мультимедиа; и

средство для идентификации местоположения частей данных медиа файла мультимедиа на основании определенного формата файла, причем средство для

идентификации местоположения части данных медиа в файле мультимедиа, содержит:

средство для преобразования выборки в порцию данных;

средство для определения смещения выборки в порции данных; и

средство для определения размеров предшествующих выборок в одной и той же порции данных; и

средство для шифрования части данных медиа;

средство для объединения зашифрованной части данных медиа с незашифрованной частью данных не медиа.

14. Устройство по п.13, в котором часть данных медиа включает в себя множество выборок аудио, и средство для шифрования части данных медиа содержит средство для шифрования части данных медиа на основе выборка аудио за выборкой аудио.

15. Устройство для воспроизведения файла мультимедиа, содержащее:

средство для выполнения синтаксического анализа файла мультимедиа, чтобы идентифицировать незашифрованную часть метаданных содержащее:

средство для определения файлового формата файла мультимедиа; и

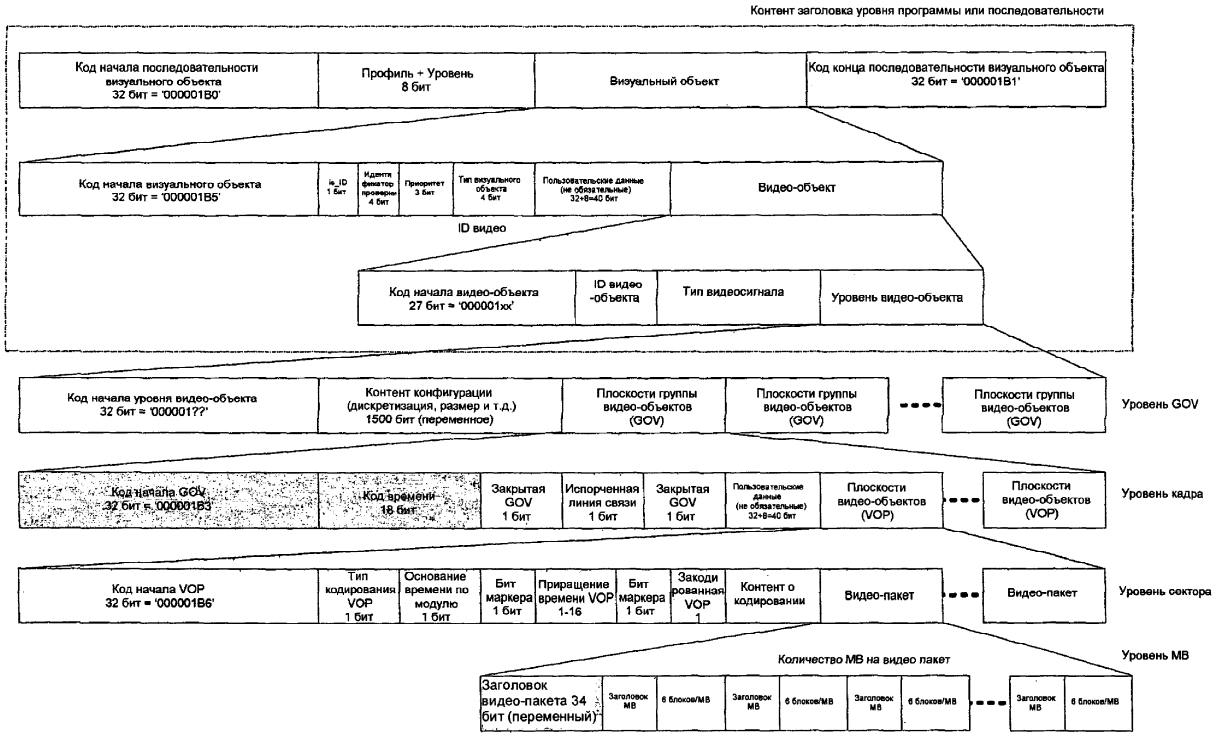
средство для идентификации незашифрованной части не медиафайла мультимедиа на основании определенного файлового формата;

средство для использования незашифрованной части метаданных, чтобы определить местонахождение позиции, представляющей интерес, в мультимедиа файле, причем позиция, представляющая интерес, имеет связанную зашифрованную часть данных медиа, причем средство для определения местонахождения выборки в медиафайле содержит:

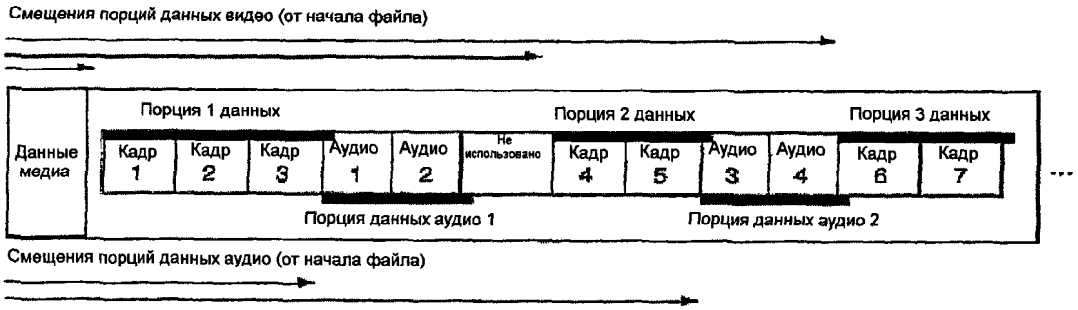
средство для преобразования выборки в порцию данных; и

средство для определения смещения выборки в порции данных; и

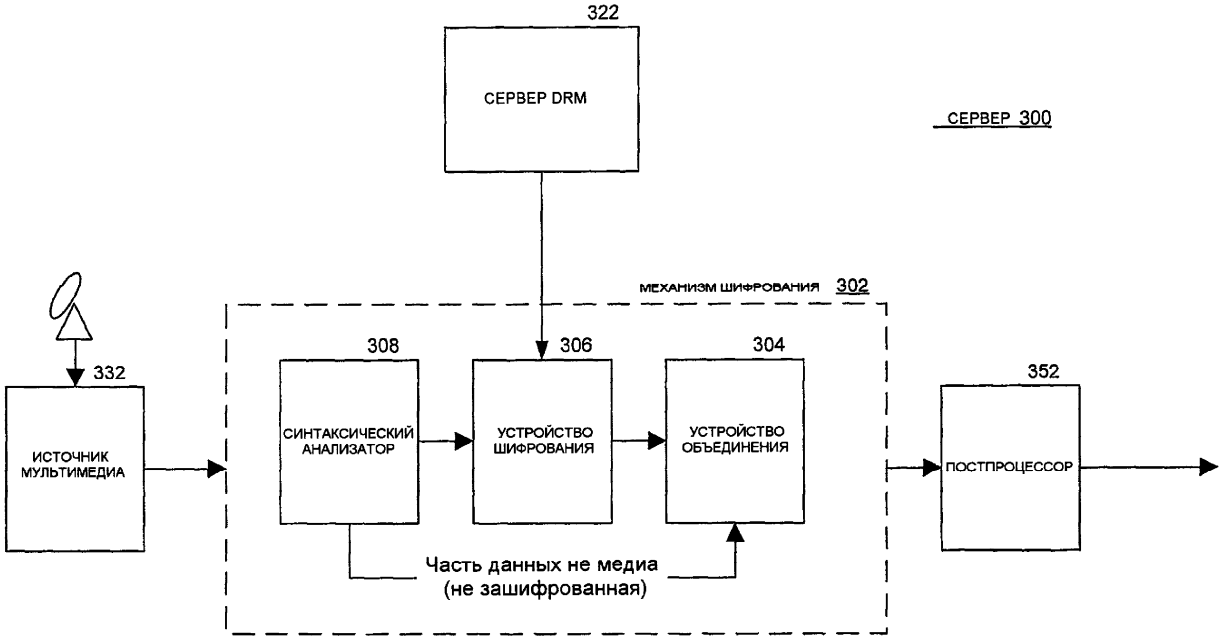
средство для дешифрования связанной зашифрованной части данных медиа.



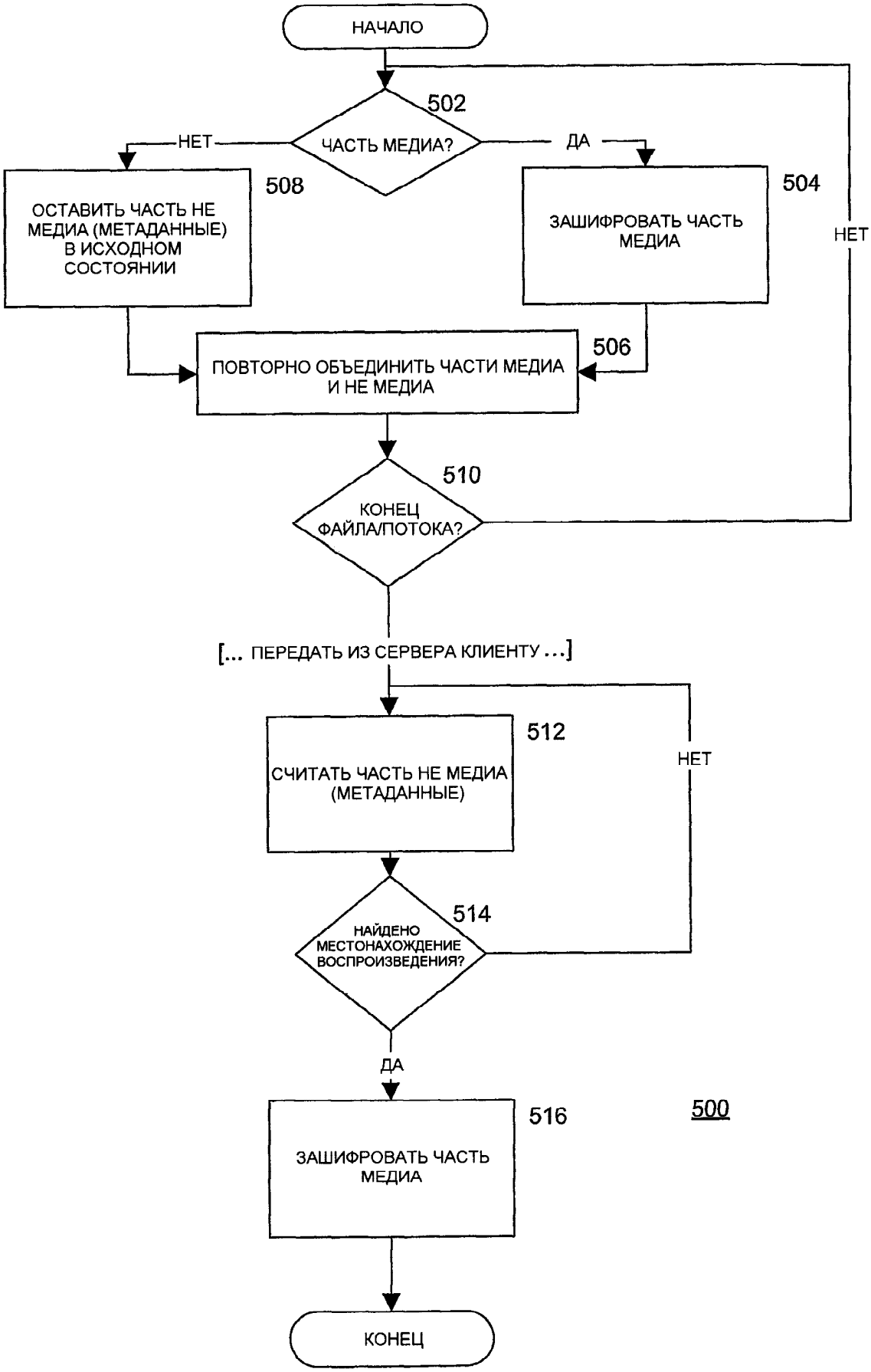
Фиг. 1



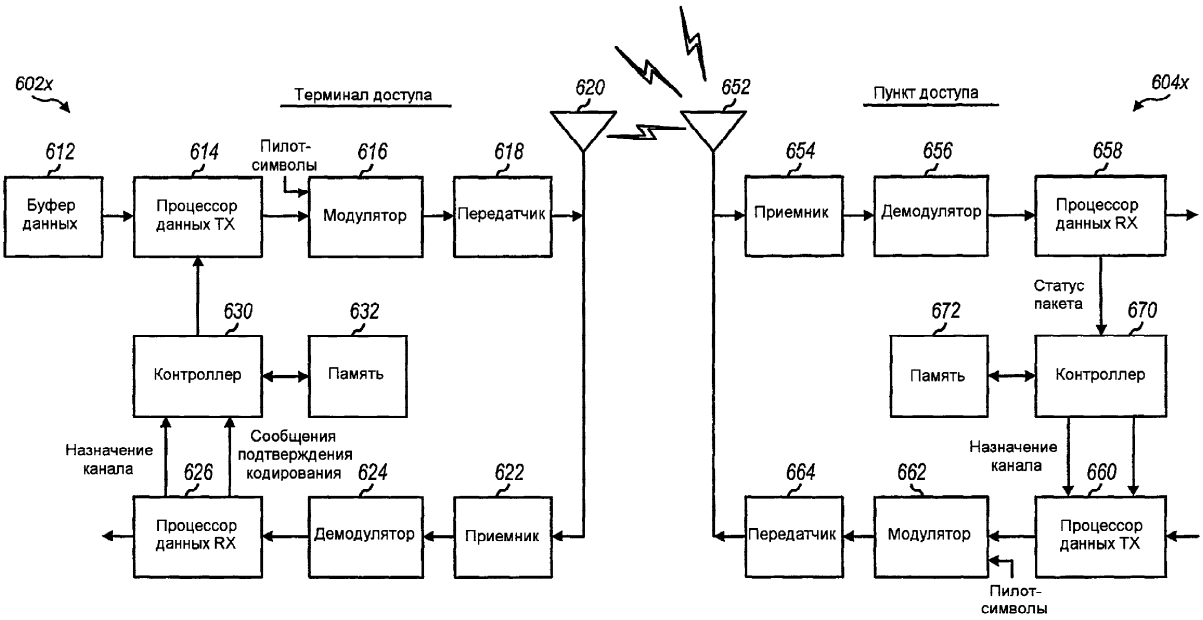
Фиг. 2



Фиг. 3


НАЧАЛО
502
ЧАСТЬ МЕДИА?
НЕТ
ДА
508
ОСТАВИТЬ ЧАСТЬ НЕ МЕДИА (МЕТАДАННЫЕ) В ИСХОДНОМ СОСТОЯНИИ
504
ЗАШИФРОВАТЬ ЧАСТЬ МЕДИА
НЕТ
506
ПОВТОРНО ОБЪЕДИНИТЬ ЧАСТИ МЕДИА И НЕ МЕДИА
510
КОНЕЦ ФАЙЛА/ПОТОКА?
[... ПЕРЕДАТЬ ИЗ СЕРВЕРА КЛИЕНТУ ...]
512
СЧИТАТЬ ЧАСТЬ НЕ МЕДИА (МЕТАДАННЫЕ)
НЕТ
514
НАЙДЕНО МЕСТОНАХОЖДЕНИЕ ВОСПРОИЗВЕДЕНИЯ?
ДА
516
ЗАШИФРОВАТЬ ЧАСТЬ МЕДИА
500
КОНЕЦ

Фиг. 5


602x
Терминал доступа
620
652
Пункт доступа
604x
612
614
Пилот-символы
616
618
654
656
658
Буфер данных
Процессор данных TX
Модулятор
Передатчик
Приемник
Демодулятор
Процессор данных RX
Статус пакета
630
632
672
670
Контроллер
Память
Память
Контроллер
Назначение канала
Сообщения подтверждения кодирования
626
624
622
664
662
660
Назначение канала
Процессор данных RX
Демодулятор
Приемник
Передатчик
Модулятор
Процессор данных TX
Пилот-символы

Фиг. 6