РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 518 392**(13) **C2**

(51) МПК
H04N 19/124 (2014.01)
H04N 21/2347 (2011.01)
H03M 13/35 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(21)(22) Заявка: **2010134365/07, 16.01.2009**

(24) Дата начала отсчета срока действия патента:
16.01.2009

Приоритет(ы):
(30) Конвенционный приоритет:
17.01.2008 EP 08300035.6;
14.02.2008 EP 08300093.5

(43) Дата публикации заявки: **27.02.2012** Бюл. № **6**

(45) Опубликовано: **10.06.2014** Бюл. № **16**

(56) Список документов, цитированных в отчете о поиске: **F. DUFAUX et al, Smart Video Surveillance System Preserving Privacy, Proceedings of the SPIE, Bellingham, vol.5685, 1 March 2005, abstract. US 2007296817 A1, 2007-12-27 . US2004028227 A1, 2004-02-12. RU 2284671 C2, 2006.09.27 . Y. WU et al, Compliant Encryption of JPEG2000 Codestreams, IEEE International Conference on Image Processing, October** (см. прод.)

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **17.08.2010**

(86) Заявка PCT:
EP 2009/050521 (16.01.2009)

(87) Публикация заявки PCT:
WO 2009/090258 (23.07.2009)

Адрес для переписки:
129090, Москва, ул.Б.Спасская, 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры", пат.пов. А.В.Миц, рег.N 364

(72) Автор(ы):
МАССУДИ Айуб (FR),
ЛЕФЕВР Фредерик (FR),
ДЮРАН Алан (FR)

(73) Патентообладатель(и):
ТОМСОН ЛАЙСЕНСИНГ (FR)

(54) СПОСОБ И УСТРОЙСТВО ДЛЯ ВЫБОРОЧНОГО ШИФРОВАНИЯ ДАННЫХ

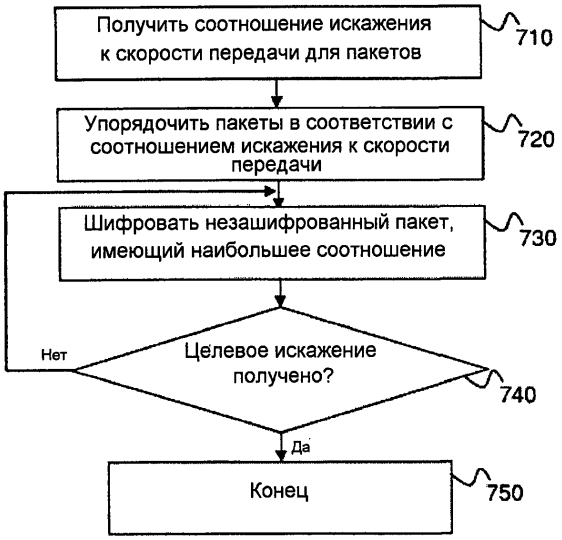
(57) Реферат:

Изобретение относится к шифрованию данных и конкретно к шифрованию данных изображения, организованных в потоки битов. Техническим результатом является обеспечение возможности адаптации к различного рода приложениям и минимизирование количества данных для шифрования, при этом максимально увеличивая защиту зашифрованного контента. Указанный технический результат достигается тем, что многослойный аудиовизуальный поток (CNT') пакетных данных, такой как получаемый кодировщиком (810) JPEG2000, принимается вместе с информацией (метаданными) о вкладе каждого пакета в снижение искажения

RU 2518392 C2

RU 2518392 C2

изображения. Вычисляется (710) соотношение искажения к скорости передачи для каждого пакета и пакеты упорядочиваются (720) по убыванию соотношения. Незашифрованный пакет, имеющий наибольшее соотношение, шифруется (730) до тех пор, пока не будет получено целевое искажение. 2 н. и 4 з.п. ф-лы, 8 ил.



ФИГ.7

(56) (продолжение):
2004, abstract . F. DUFAUX et al, Video surveillance using JPEG2000, Applications of Digital Image Processing XXVII, vol.5558, November 2004, abstract. WEI WANG et al, Research Article Energy-Constrained Quality Optimization for Secure Image Transmission in Wireless Sensor Networks, Hindawi Publishing Corporation Advances in Multimedia Volume 2007, Issue 1, January 2007, abstract. ANDREAS POMMER, et al, Selective Encryption of Wavelet-Packet encoded Image Data Efficiency and Security, Multimedia Systems, vol.9, N3, Springer-Verlag, 2003, abstract

RU 2518392 C2

RU 2518392 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 518 392** (13) **C2**

(51) Int. Cl.
H04N 19/124 (2014.01)
H04N 21/2347 (2011.01)
H03M 13/35 (2006.01)

(12) ABSTRACT OF INVENTION

(21)(22) Application: **2010134365/07, 16.01.2009**

(24) Effective date for property rights:
16.01.2009

Priority:
(30) Convention priority:
17.01.2008 EP 08300035.6;
14.02.2008 EP 08300093.5

(43) Application published: **27.02.2012** Bull. № **6**

(45) Date of publication: **10.06.2014** Bull. № **16**

(85) Commencement of national phase: **17.08.2010**

(86) PCT application:
EP 2009/050521 (16.01.2009)

(87) PCT publication:
WO 2009/090258 (23.07.2009)

Mail address:
129090, Moskva, ul.B.Spasskaja, 25, stroenie 3, OOO "Juridicheskaja firma Gorodisskij i Partnery", pat.pov. A.V.Mits, reg.N 364

(72) Inventor(s):
MASSUDI Ajub (FR),
LEFEVR Frederik (FR),
DJuRAN Alan (FR)

(73) Proprietor(s):
TOMSON LAJSENSING (FR)

RU 2518392 C2

(54) METHOD AND APPARATUS FOR SELECTIVE DATA ENCRYPTION

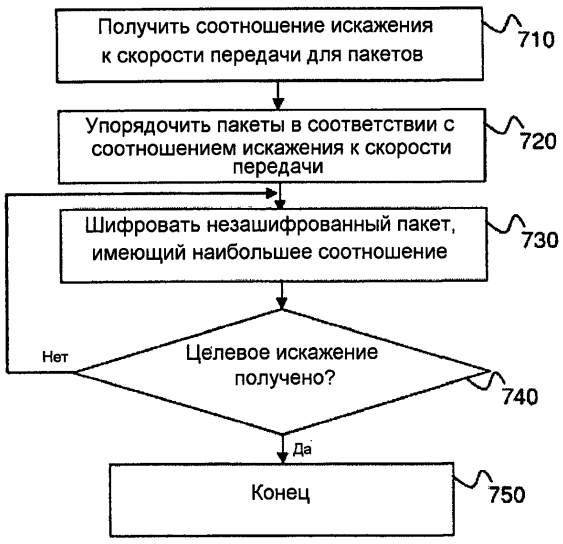
(57) Abstract:

FIELD: radio engineering, communication.

SUBSTANCE: invention relates to data encryption and specifically to encryption of image data organised into bit streams. A layered audiovisual packet data stream (CNT'), such as one obtained by a JPEG2000 encoder (810), is received together with information (metadata) about the contribution of each packet to the reduction of image distortion. The distortion-to-rate ratio for each packet is calculated (710) and the packets are ordered (720) in descending ratio. The non-encrypted packet having the highest ratio is encrypted (730) until the target distortion is obtained.

EFFECT: facilitating adaptation to a different type of applications and minimising the amount of data for encryption, while maximising protection of the encrypted content.

6 cl, 8 dwg



ФИГ.7

RU 2518392 C2

ОБЛАСТЬ ТЕХНИКИ, К КОТОРОЙ ОТНОСИТСЯ ИЗОБРЕТЕНИЕ

Настоящее изобретение относится, в целом, к шифрованию данных и, конкретно, к шифрованию данных изображения, организованных в потоки битов.

УРОВЕНЬ ТЕХНИКИ

Данный раздел предназначен ознакомить читателя с различными аспектами области техники, которые могут относиться к различным аспектам настоящего изобретения, которые описаны и/или заявлены ниже. Полагается, что это обсуждение будет полезным для предоставления пользователю информации о предпосылках, чтобы способствовать лучшему пониманию различных аспектов настоящего изобретения. Соответственно, должно быть понятно, что эти положения должны толковаться в этом свете, а не в качестве допущений известного уровня техники.

Давно известна защита видеоданных посредством шифрования, особенно в телевизионных системах условного доступа. Фигура 1 иллюстрирует традиционный подход известного уровня техники к управлению доступом к контенту. Сначала видеосигнал CNT кодируется 110, используя стандартный кодировщик сжатия, а полученный поток CNT' битов затем шифруется 120, используя стандарт симметричного шифрования (такой как DES, AES или IDEA). Зашифрованный поток [CNT'] битов затем принимается ресивером, который расшифровывает 130 зашифрованный поток [CNT'] битов для того, чтобы получить закодированный поток CNT' битов, который декодируется 140 для того, чтобы получить видеосигнал CNT, то есть, по меньшей мере, в теории, идентичный исходному видеосигналу. В данном подходе, называемом полностью многослойным, сжатие и шифрование являются полностью независимыми процессами. Аудиовизуальный поток битов обрабатывается в качестве классических данных открытого текста с предположением, что все символы или биты открытого текста являются одинаковой значимости.

Данная схема является уместной, когда передача контента не связана ограничениями, но она кажется неадекватной в ситуациях, где ресурсы (такие как память, возможности производительности и вычисления) ограничены. Более глубокие исследования показывают особые характеристики контента изображения и видео: высокую скорость передачи данных и ограниченную разрешенную полосу пропускания, которые объясняют неадекватность стандартной технологии шифрования для такого контента. Это привело исследователей к тому, чтобы изучать новые схемы организации защиты контента - названные «выборочным шифрованием», «неполным шифрованием», «гибким шифрованием» или «перцепционным шифрованием» - посредством применения шифрования к подмножеству потока битов с ожиданием того, что получающийся частично зашифрованный поток битов бесполезен без расшифровки зашифрованного подмножества. Основной подход в том, чтобы разделить контент на две части: первая часть является основной частью сигнала (например, коэффициенты постоянного тока, DC, при разложении согласно Дискретному Косинусному Преобразованию, DCT, или низкочастотный уровень при разложении согласно Дискретному Вейвлет-Преобразованию, DWT,), которая дает возможность воссоздания четкого варианта исходного сигнала, но с низким качеством, и вторая часть, которая может быть названа частью «расширения» (например, коэффициенты переменного тока, AC, в DCT-разложении изображения или высокочастотные слои в DWT), которая дает возможность восстановления тонких деталей изображения и воссоздания варианта исходного сигнала с высоким качеством. В соответствии с новой схемой шифруется только основная часть, в то время как часть расширения передается незашифрованной или, в некоторых случаях, с легкой перестановкой элементов. Целью является защитить контент, а не сам поток

двоичных данных.

Фигура 2 иллюстрирует выборочное шифрование в соответствии с известным уровнем техники. Кодирование и декодирование выполняется так же, как на Фигуре 1. В выборочном шифровании, закодированный поток CNT' битов шифруется 220 в зависимости от параметров 240 выборочного шифрования. Эти параметры могут, как упоминалось, например, устанавливать, что должен быть зашифрован только коэффициенты DC или низкочастотный слой, в то время как оставшаяся часть закодированного потока CNT' битов должна быть оставлена незашифрованной. Частично зашифрованный поток [CNT'] битов затем (частично) расшифровывается 230 в зависимости от параметров 240 выборочного шифрования.

Нижеследующие критерии важны для оценки любого алгоритма выборочного шифрования и будут использованы для изучения алгоритмов известного уровня техники:

• Возможность настройки: алгоритм выборочного шифрования с возможностью настройки дает возможность изменения параметров шифрования, что может быть желаемой характеристикой.

• Визуальная деградация: оценивает, насколько зашифрованное изображение искажено в сравнении с обычным изображением. В некоторых приложениях может быть желательной низкая визуальная деградация для того, чтобы клиенты имели искаженный, но видимый контент, так как это разрешает предварительный просмотр, в то время как другие приложения могут требовать сильную визуальную деградацию.

• Криптографическая защита: дает возможность измерить, насколько сложно взломать алгоритм. Безопасность алгоритма отчасти основывается на ключе шифрования, но полезно, чтобы зашифрованная часть не была или была тяжело предсказуема из незашифрованной части.

• Сокращение шифрования: дает соотношение зашифрованной части ко всем данным. Эффективный алгоритм преимущественно минимизирует это соотношение.

• Совместимость/возможность перекодировки формата: предпочтительным является, чтобы зашифрованный поток битов был совместим с форматом сжатия, используемым для формирования сжатого потока битов, и чтобы любой стандартный декодер имел возможность декодировать зашифрованный поток битов без расшифровки.

• Дружественность сжатию: алгоритм выборочного шифрования считается дружественным сжатию, если он не оказывает или оказывает незначительное влияние на эффективность сжатия.

• Устойчивость к ошибкам: указывает желаемую характеристику, что алгоритм выборочного шифрования не порождает ошибки передачи, и/или что он сохраняет устойчивость кодировщика к ошибкам.

Дополнительно, так как известный уровень техники представляется сфокусированным на JPEG2000, который также будет использован в качестве неограничивающего варианта осуществления изобретения, теперь будет дано краткое введение в соответствующие части этого стандарта, т.е. его структуру потока кода.

Поток кода JPEG2000 организован в пакеты, пакеты потока кода являются элементарными единицами, которые переносят данные конкретных комбинаций объектов, называемых Разрешение, Слой, Компонент и Граница. Сжатое изображение с R разрешениями, L слоями, P границами и C компонентами, таким образом, образует RxLxCxP пакеты. Должно быть отмечено, что EBCOT (Вложенное Блочное Кодирование с Оптимизированным Усечением) функция кодировщика JPEG2000 имеет возможность предоставлять информацию, относящуюся к соотношению искажения к скорости передачи каждого пакета.

JPEG2000 использует вложенный поток битов: поток кода может быть усечен на любом заданном пакете без неблагоприятного влияния на ранее закодированные.

Фигура 3 иллюстрирует основную структуру потока кода, содержащую:

• Основной заголовок 310, содержащий маркерный сегмент 312 потока Начала Кода (SOC = 0xFF4F) и маркерные сегменты 314 основного заголовка. Маркер SOC указывает начало потока кода и необходим в качестве первого маркера. Маркерные сегменты основного заголовка указывают много параметров сжатия, определенные пользователем, такие как, например, порядок прогрессии, стиль основного кодирования, стиль кодирования компонентов и размер области изображения.

• Один или более заголовки части области 320a, 320b, каждый содержащий маркер 322 Начала части Области (SOT = 0xFF90), информацию части области 324a, 324b, и маркер 326 Начала Данных (SOD = 0xFF93). Как должно быть принято во внимание, SOT 322 и SOD 326 имеют стандартные значения, в то время как информация 324a, 324b части области содержит информацию об области; например информация 324a части области указывает, что она принадлежит Области 0, в то время как информация 324b части области указывает, что она принадлежит к Области 1. По меньшей мере, один заголовок 320a, 320b части области необходим в начале каждой части области, которая содержит заголовок 320a, 320b части области и, как правило, следующий поток 330a, 330b битов, где маркер SOD указывает начало потока 330a, 330b битов, который несет в себе сжатые данные.

• Поток 340 Конца Кода: этот маркер (EOC = 0xFF9) указывает конец потока кода.

Должно быть отмечено, что для данных пакета некоторые кодовые слова - те, что в диапазоне [0xFF90; 0xFFFF] - в JPEG2000 зарезервированы. Такие зарезервированные кодовые слова используются в качестве маркеров и маркерных сегментов, которые разделяют главные компоновочные блоки потока. Например, такими зарезервированными кодовыми словами являются SOT (0xFF90), SOD (0xFF93) и EOC (0xFFD9). Во время шифрования потока кода важно убедиться, что «нормальные» (т.е. незарезервированные) кодовые слова не превратятся в зашифрованные кодовые слова, значения которых зарезервированы.

Как может быть видно, поток битов в основном составлен из заголовков пакета и данных пакета, которые образуют пакеты. Фигура 4 иллюстрирует характерный пакет JPEG2000, содержащий заголовок 420 пакета и данные 440 пакета. Заголовки пакета могут использоваться в потоке битов или в основном заголовке в зависимости от опций, определенных пользователем. Фигура 4 показывает использование таких заголовков: заголовок 410 Начала Пакета (SOP = 0xFF91) и Заголовок 430 Конца Пакета (EPH = 0xFF92) соответственно указывают начало и конец заголовка 420 пакета.

Заголовок 420 пакета содержит информацию, необходимую декодеру для того, чтобы корректно проанализировать и декодировать данные пакета:

• Пакет нулевой длины: указывает является или нет данный пакет пустым.

• Включение блока кода: для каждой границы, древовидная схема тэга, используется для кодирования информации включения для включенных блоков кода.

• Информация нулевой битовой плоскости: для каждой границы, древовидная схема тэга кодирует первую не нулевую битовую плоскость.

• Число проходов кодирования: Кодовые слова стиля Huffman используются для кодирования числа проходов кодирования включенного для каждого блока кода.

• Длина сжатых данных от каждого блока кода.

• В “Techniques for a Selective Encryption of Uncompressed and Compressed Images”, Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Гент, Бельгия,

Сентябрь 9-11, 2002, M. Van Droogenbroeck и R. Benedett предложили кодировщику JPEG Huffman завершать серии нулей кодовыми словами/символами для того, чтобы повысить энтропию. Добавленные биты добавляются к таким словам для того, чтобы более полно указывать размеры и знаки ненулевых коэффициентов, и только эти добавленные биты шифруются, используя DES или IDEA. Используя установленные выше критерии, решение оценивается следующим образом:

• Возможность настройки: Этот способ не предлагает возможность настройки.

• Визуальная деградация: достигается приемлемый уровень визуальной деградации.

• Криптографическая защита: около 92% данных зашифровано, используя безопасный симметричный шифр и действительно очень трудно разрушить алгоритм шифрования или попытаться предугадать зашифрованную часть.

• Сокращение шифрования: Для достижения достаточного уровня визуальной деградации было определено, что не больше 5 коэффициентов должны быть оставлены незашифрованными. Это приводит к тому, что зашифрованная часть составляет 92%, что относительно велико.

• Совместимость/возможность перекодировки формата: JPEG совместимый.

• Дружественность сжатию: Шифрование отделено от кодировщика Huffman и не оказывает влияния на эффективность сжатия.

• Устойчивость к ошибкам: лавинообразное воздействие DES алгоритма из единичной битовой ошибки порождает многочисленные битовые ошибки, таким образом, этот алгоритм шифрования не сохраняет устойчивость к ошибкам.

В “Selective Encryption of Wavelet-Packet Encoded Image Data”, ACM Multimedia Systems Journal, Special Issue on Multimedia Security в 2003, A. Pommer и A. Uhl предложили алгоритм на основе AES шифрования информации заголовка кодирования вейвлет пакета изображения, заголовок, устанавливающий древовидную структуру поддиапазона. Используя установленные выше критерии, решение оценивается следующим образом:

• Возможность настройки: параметры шифрования статичные, возможность настройки отсутствует.

• Визуальная деградация: 100%; зашифрованный контент не может быть просмотрен без расшифровки.

• Криптографическая защита: Не защищает от выбранной атаки открытого текста, так как статистические свойства вейвлет коэффициентов защищены шифрованием, так что поддиапазон аппроксимации может быть воссоздан. Это даст взломщику размер поддиапазона аппроксимации (более низкое разрешение) и затем могут быть воссозданы смежные поддиапазоны, так как близкие поддиапазоны содержат высококоррелированные коэффициенты.

• Сокращение шифрования: высокое сокращение в шифровании; древовидная структура поддиапазона представляет небольшую часть в вейвлет кодировании.

• Совместимость/возможность перекодировки формата: не совместим; наоборот, он предполагает, что кодировщик не использует стандартную декомпозицию вейвлет пакета.

• Дружественность сжатию: древовидная схема поддиапозона является сформированной псевдослучайно, что неблагоприятно воздействует на дружественность сжатию.

• Устойчивость к ошибкам: лавинообразное воздействие AES алгоритма из единичных битовых ошибок порождает многочисленные битовые ошибки.

На “Compliant Encryption of JPEG2000 Codestreams”, IEEE International Conference on

Image Processing (ICIP 2004), Сингапур, Октябрь 2004, Y. Wu и R. H. Deng предложили совместимый с JPRG2000 алгоритм шифрования, который многократно шифрует Вклад Кода Блока в Пакеты (CCP). Процессы шифрования действуют на CCP (в данных пакета), используя шифры потока или шифры блока, предпочтительно шифры потока с добавлением модуля арифметики. Ключевой поток формируется, используя Шифр Райвеста 4 (RC4). Каждый CCP многократно шифруется до тех пор, пока у него не останется запрещенных кодовых слов (т.е. любое слово в диапазоне [0xFF90, 0xFFFF]). Используя установленные выше критерии, решение оценивается следующим образом:

• Возможность настройки: не настраиваемый.

• Визуальная деградация: переменная; зависит от числа зашифрованных CCP.

• Криптографическая защита: зависит от числа зашифрованных CCP. Тем не менее, возможная необходимость многочисленных повторений для того, чтобы получить соответствующий поток кода, может дать информацию для атак побочного канала.

• Сокращение шифрования: Шифрование многократно повторяющееся, таким образом может потребоваться много повторов для того, чтобы получить соответствие, в особенности для больших CCP, где едва ли не половину зашифрованных CCP необходимо шифровать более одного раза для того, чтобы получить соответствие.

• Совместимость/возможность перекодировки формата: полностью совместим с JPEG2000.

• Дружественность сжатию: нет влияния на сжатие.

• Устойчивость к ошибкам: Алгоритм шифрования основан на блоках; любая ошибка в заданном бите в зашифрованном потоке битов будет распространяться на многие другие биты, что привносит сильное искажение на расшифрованное изображение.

В “Selective Encryption of the JPEG2000 Bitstream”, Journal of Electronic Imaging -- Октябрь - Декабрь 2006 -- Том 15, Выпуск 4, 043013, R. Norcen and A. Uhl отмечают, что JPEG2000 является вложенным потоком битов, и что наиболее важные данные отправляются в начале потока битов. На основании этого предлагаемая схема состоит из AES шифрования выбранных данных пакета. Алгоритм использует два дополнительных маркера SOP и EPH (как проиллюстрировано на Фигуре 5) для того, чтобы идентифицировать данные пакета. Затем эти данные пакета шифруются, используя AES в режиме CFB, так как данные пакета имеют переменную длину. Эксперименты проводились на двух видах изображений (сжатых с потерями и без), с различными порядками прогрессии (порядки прогрессии разрешения и слоя). Оценочным критерием была визуальная деградация, получаемая для заданной величины зашифрованных данных. Было обнаружено, что для изображений, сжатых с потерями, прогрессия слоя дает лучшие результаты. Для изображений, сжатых без потерь, прогрессия разрешения дает лучшие результаты.

• Возможность настройки: ненастраиваемый.

• Визуальная деградация: высокая визуальная деградация достижима путем шифрования 20% данных.

• Криптографическая защита: не адресуется авторам, которые основывают свою оценку защиты на визуальной деградации, которая не является надежным критерием защиты.

• Сокращение шифрования: 20% данных шифруются для того, чтобы достичь приемлемого уровня визуальной деградации.

• Совместимость/возможность перекодировки формата: не совместим с JPEG2000.

• Дружественность сжатию: нет влияния на сжатие.

• Устойчивость к ошибкам: предлагаемая схема основана на AES в режиме CFB.

Этот цепной режим из ошибок в зашифрованном тексте порождает после расшифровки много ошибок в открытом тексте.

Как будет видно, решения известной области техники имеют определенные недостатки:

• Возможность настройки: Решения предлагают статичные алгоритмы шифрования. Основной недостаток этих подходов в том, что зашифрованная часть не оптимизирована для того, чтобы снизить количество шифруемых данных и максимально увеличить защиту контента.

• Визуальная деградация: Желательно иметь настраиваемый алгоритм, который позволяет иметь многоуровневую визуальную деградацию.

• Криптографическая защита: Во многих решениях этот критерий вообще не берется в расчет, и только визуальная деградация используется в качестве критерия защиты, что недостаточно, так как многие алгоритмы добиваются важной визуальной деградации, но слабой криптографической защиты.

• Сокращение шифрования: в то время как некоторые решения добиваются значительного сокращения шифрования, другие не добиваются.

• Совместимость/возможность перекодировки формата: Многие решения не рассматривают эту проблему во время разработки их алгоритма выборочного шифрования. Таким образом, зашифрованный поток битов не может быть расшифрован стандартным декодером.

• Дружественность сжатию: некоторые алгоритмы выборочного шифрования используют очень большие ключи шифрования или привносят значительное увеличение размера файла.

• Устойчивость к ошибкам: Это свойство редко рассматривается в литературе. В сетях склонных к возникновению ошибки, очень желательно чтобы алгоритм шифрования не порождал ошибки или неблагоприятно влиял на технологии устойчивости к ошибкам кодировщика.

По этой причине должно быть принято во внимание, что существует необходимость гибкого решения, которое дает возможность адаптации к различного рода приложениям и минимизирует количество данных для того, чтобы шифровать, при этом максимально увеличивая защиту зашифрованного контента. Это изобретение предоставляет такое решение.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

В первом аспекте изобретение направлено на способ защиты аудиовизуального контента организованного в пакеты. Защищается незащищенный пакет с наибольшим соотношением искажения к скорости передачи; и этот этап защиты повторяется до тех пор, пока не будет получен предопределенное искажение аудиовизуального контента.

В соответствии с первым предпочтительным вариантом осуществления, способ дополнительно содержит упредительный этап вычисления соотношения искажения к скорости передачи пакетов. Для снижения искажения изображения благоприятно, что способ содержит упредительный этап вычисления вклада каждого пакета.

В соответствии со вторым предпочтительным вариантом осуществления, способ дополнительно содержит этап выбора, по меньшей мер, одной части пакета для защиты.

В соответствии с третьим предпочтительным вариантом осуществления, способ дополнительно содержит этап вывода зашифрованного аудиовизуального контента и информации о том какие пакеты защищены.

В соответствии с четвертым предпочтительным вариантом осуществления, способ дополнительно содержит этап сортировки пакетов в соответствии с их соотношением

искажения к скорости передачи.

В соответствии с пятым предпочтительным вариантом осуществления, этап защиты содержит шифрование незащищенного пакета.

В соответствии с шестым предпочтительным вариантом осуществления, этап защиты содержит замещение данных в незащищенном пакете фиктивными данными.

Во втором аспекте, изобретение направлено на обеспечение устройства для защиты аудиовизуального контента, организованного в пакеты. Упомянутое устройство включает в себя устройство защиты, выполненное с возможностью защищать незащищенный пакет с наибольшим соотношением искажения к скорости передачи; и повторять этап защиты до тех пор, пока не будет получено предопределенное искажение аудиовизуального контента.

В соответствии с первым предпочтительным вариантом осуществления, устройство защиты выполнено с возможностью защищать незащищенный пакет путем использования шифрования.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

Предпочтительные признаки настоящего изобретения теперь будут описаны в виде не накладывающего ограничения примера, со ссылкой на прилагаемые чертежи, на которых:

Фигура 1 иллюстрирует традиционный подход известного уровня техники для управления доступом к контенту;

Фигура 2 иллюстрирует выборочное шифрование в соответствии с известным уровнем техники;

Фигура 3 иллюстрирует структуру основного потока кода JPEG2000 известного уровня техники;

Фигура 4 иллюстрирует характерный пакет JPEG2000 известного уровня техники;

Фигура 5 иллюстрирует основную идею изобретения;

Фигура 6 иллюстрирует предпочтительный вариант осуществления выборочного шифрования в соответствии с изобретением;

Фигура 7 иллюстрирует способ для оптимального выбора пакета в соответствии с предпочтительным вариантом осуществления изобретения;

Фигура 8 иллюстрирует устройство для шифрования и устройство для расшифровки в соответствии с предпочтительным вариантом осуществления изобретения.

ПРЕДПОЧТИТЕЛЬНЫЙ ВАРИАНТ ОСУЩЕСТВЛЕНИЯ ИЗОБРЕТЕНИЯ

Фигура 5 иллюстрирует основную идею изобретения: введение нового процесса, называемого «динамическим выбором данных». Для заданного входного сжатого потока CNT' битов, выбирается 540 набор параметров шифрования. С выбранным набором параметров шифрования и сжатым потоком CNT' битов пакеты для шифрования динамически выбираются 550 и шифруются 520 для того, чтобы сформировать зашифрованный поток [CNT'] битов.

В предпочтительном, не накладывающем ограничения, варианте осуществления, изобретение используется в системе JPEG2000. Фигура 6 иллюстрирует предпочтительный вариант осуществления выборочного шифрования в соответствии с изобретением. Сначала выбирается 610 приложение, как дополнительно будет описано здесь и далее, которое определяет параметры сжатия, такие как порядок прогрессии и число разрешений. Шифрование затем управляется числом параметров шифрования, которое зависит от выбранного приложения:

- R_e: определяет разрешения, которые необходимо зашифровать.

- L_{er}: соотношение шифрования слоев; определяет процентное соотношение слоев,

которые необходимо зашифровать.

- P_{er}: соотношение шифрования пакетов; определяет процентное соотношение байтов, которые необходимо зашифровать внутри каждого пакета.

- C_e: определяет компоненты, которые необходимо зашифровать.

- P_e: определяет границы, которые необходимо зашифровать.

Когда получены 620 параметры сжатия и параметры шифрования, выбирается 630 набор S_1 пакетов, которые являются кандидатами для шифрования. Этот набор S_1 пакетов может, например, быть пакетами разрешений, которые необходимо зашифровать. Затем, для того чтобы выбрать 640 подмножество пакетов, которые необходимо зашифровать, используются метаданные, сформированные кодировщиком JPEG2000 (и, по меньшей мере, некоторые метаданные также отправляются, возможно совместно с дополнительными данными, которые дают возможность расшифровки приемнику для того, чтобы использовать в расшифровке). Для каждого выбранного пакета затем выбираются 650 данные пакета, которые необходимо зашифровать, сопровождаемые шифрованием выбранных данных выбранных пакетов. Специалист в соответствующей области должен принять во внимание, что не всегда необходимо ждать все пакеты до начала выбора. Этапы способа, таким образом, могут преимущественно выполняться параллельно, с тем, что также относится к этапу 660 шифрования. Таким образом, может быть видно, что параметры шифрования определяют данные, которые будут зашифрованы.

Должно быть отмечено, что возможно оптимизировать шифрование пакета, необходимое для того, чтобы добиться указанного визуального искажения (или деградации). Фигура 7 иллюстрирует способ для оптимального выбора пакета. Кодировщик JPEG2000 формирует сжатое изображение, как, впрочем, и относящиеся к нему метаданные, содержащие информацию о вкладе каждого пакета в снижение искажения изображения. Это не влечет за собой какие-либо дополнительные вычисления, так как эти вычисления уже выполнены кодировщиком во время процедуры управления скоростью передачи EBCOT. Таким образом, возможно вычислить 710 соотношение искажения к скорости передачи для каждого пакета как:

$$\lambda = \frac{\partial D}{\partial r}$$

где D является искажением сжатого изображения, а r является размером закодированного потока битов, соответствующего пакету. Затем пакеты могут быть упорядочены 720 в соответствии с их соотношениями искажения к скорости передачи.

Для того чтобы добиться определенного искажения изображения, возможно начать шифрование с пакета с наибольшим отношением искажения к скорости передачи и продолжить со следующим наибольшим отношением, и так далее, до тех пор, пока не будет получено желаемое общее искажение изображения. Иными словами, незашифрованный пакет с наибольшим отношением искажения к скорости передачи шифруется 730 и, если целевое искажение получено (Y на этапе 740), то способ заканчивается 750; иначе (N на этапе 740) способ возвращается к этапу 730. Целевое искажение может быть выражено как сумма вкладов в снижение искажения зашифрованных пакетов.

Фигура 8 иллюстрирует устройство для шифрования и устройство для расшифровки в соответствии с предпочтительным вариантом осуществления изобретения. Устройство 800 шифрования содержит кодировщик 810, который предоставляет закодированный поток CNT' данных пакетов устройству 820 шифрования, как, впрочем, и метаданные,

по меньшей мере, одному процессору 840 (здесь и далее «процессор»). Процессор выполнен с возможностью вычислять соотношение искажения к скорости передачи и указывать устройству 820 шифрования (которое может быть воплощено в процессоре 840) шифровать определенные пакеты - т.е. тот (те), что имеет(ют) наибольшее соотношение искажения к скорости передачи - до тех пор, пока не будет получено целевое искажение. Специалист в соответствующей области должен принять во внимание, что существует много способов реализовать это: процессор 840 может многократно, в течение времени, указывать устройству 820 шифрования шифровать пакет, но процессор 840 также может вычислить, какой пакет шифровать так, чтобы получить целевое искажение, до момента предоставления команд шифровать все эти пакеты. Устройство 800 шифрования, таким образом, выполнен с возможностью выдавать поток [CNT'] зашифрованных и, как правило, также незашифрованных пакетов и «info» информацию, такую, как указание, какие пакеты зашифрованы, позволяя правильно расшифровать зашифрованные пакеты.

Устройство 850 расшифровки содержит процессор 860, выполненный с возможностью принимать «info» информацию, позволяющую выполнять расшифровку, и указывает устройству 870 расшифровки расшифровать определенные пакеты. Устройство 870 расшифровки выполнено с возможностью принимать поток [CNT'] пакета и использовать команды от процессора 860 для того, чтобы расшифровать пакеты, которые зашифрованы. Таким образом, формируется расшифрованный поток CNT' пакета и отправляется устройству 850 декодирования для декодирования так, чтобы получить воссозданный контент CNT. Устройство 850 расшифровки преимущественно воплощено в процессоре 860. В целях описания и формулы изобретения, «процессор» предназначен относиться в устройстве к совокупности устройств и тому подобному с вычислительными возможностями.

Другой вариант осуществления использует для защиты пакетов вместо шифрования замещение данных. В этом варианте, защита данных содержит в себе извлечение данных из пакета и установка на их месте фиктивных, предпочтительно случайных, данных. Для того чтобы снять защиту с данных, приемник запрашивает данные для защищенных пакетов (или сами исходные пакеты) и в момент предпочтительно зашифрованной доставки заменяет фиктивные пакеты принятыми данными (или защищенные пакеты принятыми пакетами).

Когда дело доходит до выбора данных пакета, которые необходимо зашифровать, должно быть принято во внимание, что не всегда необходимо шифровать целиком данные пакета для того, чтобы получить достаточный уровень защиты. В предпочтительном варианте осуществления, байты пакета сгруппированы в блоки по 16 байт. Если последний блок меньше 16 байт, он остается незашифрованным. Предпочтительный вариант осуществления использует измененный режим CTR (счетчика) алгоритма AES-128, который выдает совместимый с форматом поток битов и сохраняет устойчивость к ошибкам. Пакеты затем шифруются в зависимости от соотношения шифрования пакетов; например, если соотношение 50%, тогда в пакете шифруется только каждый второй байт.

Так как кодовые слова в диапазоне [FF90; FFFF] запрещены, измененный режим CTR использует модульное приращение вместо XOR. Для расшифровки, все операции приращения заменяются вычитанием. Алгоритм шифрования следующий (где B_k текущий байт для шифрования, $O_i[k]$ выходные данные алгоритма AES и C_k - зашифрованный байт):

- Если B_k = 0xFF, тогда не шифровать B_k.

- Иначе:

Если B_{k-1} = 0xFF, тогда $C_k = (B_k+O_i[k])$модуль[0x90],

Иначе $C_k = (B_k+O_i[k])$модуль[0xFF].

Должно быть принято во внимание, что алгоритм избегает повторения алгоритма шифрования для того, чтобы получить совместимый поток битов шифра.

Как может быть видно, параметры шифрования могут быть тонко настроены для того, чтобы получить целевую визуальную деградацию или целевую масштабируемость:

- Визуальная деградация: увеличивается с числом зашифрованных разрешений (R_e) и числом зашифрованных уровней качества (L_{er}).

- Масштабируемость разрешения: для изображения сжатого с R уровнями разрешения (R-1 уровнями декомпозиции), если желаемым размером предварительного просмотра является $X \cdot Y$ (с $X=M/2^n$, $Y=N/2^n$, $n \leq R-1$), n - наивысшие шифруемые уровни разрешения.

- Масштабируемость области пространства: конкретные области изображения могут быть выборочно зашифрованы путем указания, какие границы (P_e) шифровать.

- Масштабируемость компонента: конкретные компоненты изображения могут быть выборочно зашифрованы путем указания, какие компоненты (C_e) шифровать.

- Масштабируемость качества: Слои качества могут быть выборочно зашифрованы путем указания соотношения (L_{er}) шифрования слоев.

Динамический выбор данных может позволить минимизировать объем данных, которые необходимо зашифровать для заданного уровня защиты. Изобретение отвечает описанным выше критериям:

• Возможность настройки: оно настраиваемое, так как возможно динамически выбирать параметры шифрования для того, чтобы добиться определенной цели.

• Визуальная деградация: достижима многоуровневая визуальная деградация посредством настройки параметров шифрования, как описано выше.

• Криптографическая защита: шифрование основано на проверенном временем алгоритме (AES) и выполняется над данными пакета, которые закодированы арифметическим кодировщиком. Считается, что алгоритм в достаточной степени защищает с криптографической точки зрения, если тяжело путем вычислений декодировать арифметически закодированный поток.

• Сокращение шифрования: оптимизация выбора пакета позволяет получать требуемую визуальную деградацию целевого приложения с минимальным числом зашифрованных байтов.

• Совместимость/возможность перекодировки формата: измененный режим CTR AES-128, который мы предлагаем, выдает, совместимый с форматом, поток битов шифра, при этом предотвращая повторное шифрование. Метаданные могут быть вложены в конкретном маркерном сегменте (например, в маркерном сегменте COM) и не оказывают влияния на совместимость с форматом.

• Дружественность сжатию: Предложенный алгоритм не оказывает влияния на сжимаемость потока битов; незначительные потери вносятся включением метаданных в поток битов.

• Устойчивость к ошибкам: предложенный алгоритм шифрует каждый байт независимо; любая ошибка в потоке битов шифра скажется только на том же самом байте после расшифровки. Таким образом, искажение будет ограничено блоком кода, в который вносит свой вклад байт.

В заключение, в целях иллюстрации, будут даны несколько сценариев приложения.

Сценарий масштабируемого разрешения: заниженное разрешение предварительного просмотра делается доступным для всех пользователей (без необходимости иметь ключ расшифровки). Устанавливаются следующие параметры:

Для сжатия:

Последовательность прогрессии: PROG = RLCP или RPLC.

Число (R) разрешений: зависит от размера предварительного просмотра.

Число (L) слоев: рекомендуется устанавливать достаточное число L слоев качества для того, чтобы иметь возможность тонко настроить выборочное шифрование для правильного снижения шифрования. Для того чтобы получить высокое снижение шифрования, как правило, важно устанавливать $L \geq 10$.

Число (C) компонентов: в этом сценарии неважно.

Число (P) границ: в этом сценарии неважно. Тем не менее, выбор числа границ (или размера) влияет на эффективность сжатия.

Для выборочного шифрования:

Соотношение (L_{er}) шифрования слоев: необходимо высокое значение (≥50%), если требуется высокая визуальная деградация, и наоборот.

Соотношение (P_{er}) шифрования пакетов: необходимо высокое значение (≥50%), если требуется высокая визуальная деградация с высокой криптографической защитой, и наоборот.

Шифруемые разрешения (R_e): Дает список разрешений, которые необходимо зашифровать. В этом сценарии будут зашифрованы только некоторое число высоких разрешений.

Шифруемые границы (P_e): все границы являются кандидатами для шифрования.

Шифруемые компоненты (C_e): все компоненты являются кандидатами для шифрования.

Сценарий масштабируемого качества: сниженное качество предварительного просмотра делается доступным для всех пользователей (без необходимости иметь ключ расшифровки). Устанавливаются следующие параметры:

Для сжатия:

Последовательность прогрессии: PROG = LRCP.

Число (R) разрешений: в этом сценарии неважно. Тем не менее, оно влияет на эффективность сжатия.

Число (L) слоев: рекомендуется устанавливать достаточное число L слоев качества для того, чтобы иметь возможность тонко настроить выборочное шифрование для правильного снижения шифрования. Для того чтобы получить высокое снижение шифрования, как правило, важно устанавливать $L \geq 10$.

Число (C) компонентов: в этом сценарии неважно.

Число (P) границ: в этом сценарии неважно. Тем не менее, выбор числа границ (или размера) влияет на эффективность сжатия.

Для выборочного шифрования:

Соотношение (L_{er}) шифрования слоев: В этом сценарии требуется оставить незашифрованными число слоев базового качества и зашифровать слои улучшенного качества. Шифруются слои улучшенного качества с самыми низкими L_{er} %.

Соотношение (P_{er}) шифрования пакетов: необходимо высокое значение (≥50%), если требуется высокая визуальная деградация с высокой криптографической защитой, и

наоборот.

Число (R_e) шифруемых разрешений: $1 \leq R_e \leq R$, требуется высокое R_e, если необходима высокая визуальная деградация.

Шифруемые границы (P_e): все границы являются кандидатами для шифрования.

Шифруемые компоненты (C_e): все компоненты являются кандидатами для шифрования.

Сценарий выборочного пространственного шифрования: конкретная область изображения должна быть зашифрована. Устанавливаются следующие параметры:

Для сжатия:

Последовательность прогрессии: PROG = PCRL.

Число (R) разрешений: в этом сценарии неважно. Тем не менее, оно влияет на эффективность сжатия.

Число (L) слоев: рекомендуется устанавливать достаточное число L слоев качества для того, чтобы иметь возможность тонко настроить выборочное шифрование для правильного снижения шифрования. Для того чтобы получить высокое снижение шифрования, как правило, его важно установить.

Число (C) компонентов: в этом сценарии неважно.

Число (P) границ: должно быть определено для того, чтобы добиться целевой пространственной степени детализации. Чем меньше границы, тем более точным будет пространственный выбор. С другой стороны, маленькие границы неблагоприятно влияют на эффективность сжатия.

Для выборочного шифрования:

Соотношение (L_{er}) шифрования слоев: необходимо высокое значение, если требуется высокая визуальная деградация, и наоборот.

Соотношение (P_{er}) шифрования пакетов: необходимо высокое значение ($\geq 50\%$), если требуется высокая визуальная деградация с высокой криптографической защитой, и наоборот.

Число (R_e) шифруемых разрешений: $1 \leq R_e \leq R$, требуется высокое R_e, если необходима высокая визуальная деградация.

Шифруемые границы (P_e): P_e содержит в себе все границы, которые охватывают любую часть, включенную в область, которую необходимо зашифровать.

Шифруемые компоненты (C_e): все компоненты являются кандидатами для шифрования.

Сценарий выборочного шифрования компонента: подмножество компонентов изображения должно быть зашифровано. Устанавливаются следующие параметры:

Для сжатия:

Последовательность прогрессии: PROG = CPRL.

Число (R) разрешений: в этом сценарии неважно. Тем не менее, оно влияет на эффективность сжатия.

Число (L) слоев: рекомендуется устанавливать достаточное число L слоев качества для того, чтобы иметь возможность тонко настроить выборочное шифрование для правильного снижения шифрования. Для того чтобы получить высокое снижение шифрования, как правило, важно установить $L \geq 10$.

Число (C) компонентов: зависит от класса/природы изображения. Например, некоторые медицинские изображения содержат огромное число компонентов.

Число (P) границ: в этом сценарии неважно. Тем не менее, оно влияет на

эффективность сжатия.

Для выборочного шифрования:

Соотношение (L_{er}) шифрования слоев: необходимо высокое значение (≥50%), если требуется высокая визуальная деградация, и наоборот.

Соотношение (P_{er}) шифрования пакетов: необходимо высокое значение (≥50%), если требуется высокая визуальная деградация с высокой криптографической защитой, и наоборот.

Число (R_e) шифруемых разрешений: $1 \leq R_e \leq R$, требуется высокое R_e, если необходима высокая визуальная деградация.

Шифруемые границы (P_e): все границы являются кандидатами для шифрования.

Шифруемые компоненты (C_e): C_e содержит в себе индексы компонентов, которые необходимо зашифровать.

Сценарий полного шифрования: требуется полное шифрование изображения. Устанавливаются следующие параметры:

Для сжатия:

Последовательность прогрессии: PROG в этом сценарии неважна; она может быть определена пользователем.

Число (R) разрешений: в этом сценарии неважно; оно может быть определено пользователем.

Число (L) слоев: в этом сценарии неважно; оно может быть определено пользователем.

Число (C) компонентов: в этом сценарии неважно; оно может быть определено пользователем.

Число (P) границ: в этом сценарии неважно; оно может быть определено пользователем.

Для выборочного шифрования:

Соотношение (L_{er}) шифрования слоев: $L_{er}=100\%$

Соотношение (P_{er}) шифрования пакетов: $P_{er}=100\%$

Число (R_e) шифруемых разрешений: $R_e=R$

Шифруемые границы (P_e): все границы являются кандидатами для шифрования.

Шифруемые компоненты (C_e): все компоненты являются кандидатами для шифрования.

Каждый признак, раскрытый в описании и (где соответствует) формуле изобретения и чертежах, может быть предоставлен независимо или в соответствующей комбинации. Описанные признаки, как осуществленные в аппаратном обеспечении, так же могут быть осуществлены в программном обеспечении, и наоборот. Связи, где применимо, могут быть осуществлены в качестве беспроводных связей или проводных, при этом необязательно являются непосредственными или выделенными связями.

Должно быть принято во внимание, что настоящее изобретение не ограничено предпочтительным вариантом осуществления, JPEG2000, но может быть равноценно использовано в других системах, имеющих схожую, многослойную архитектуру сжатого изображения, и в которой кодировщик предоставляет информацию о снижении искажения каждого пакета.

Ссылочные цифровые обозначения, встречающиеся в формуле изобретения, служат только в качестве иллюстрации и не должны иметь ограничивающего воздействия на объем формулы изобретения.

Формула изобретения

1. Способ защиты сжатого аудиовизуального контента, организованного в набор пакетов, содержащий этапы, на которых: вычисляют (710) соотношение искажения к скорости передачи для каждого пакета в наборе пакетов; шифруют (660) незащищенный пакет с наибольшим соотношением искажения к скорости передачи из набора пакетов; и повторяют этап шифрования только до тех пор, пока не будет получено предопределенное искажение аудиовизуального контента.

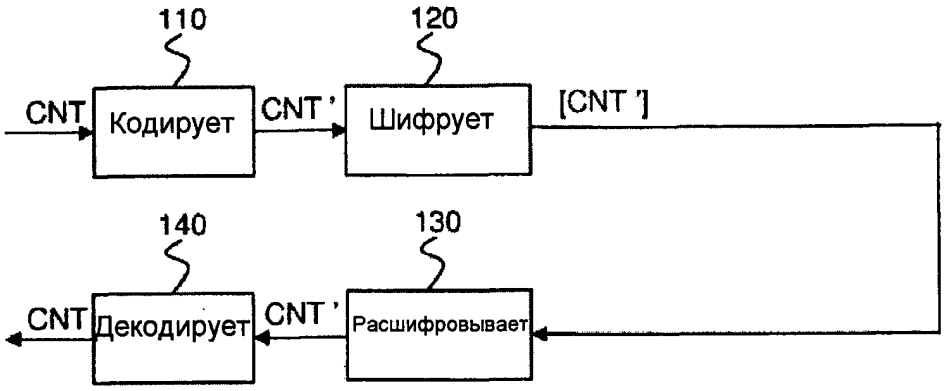
2. Способ по п.1, дополнительно содержащий упредительный этап, на котором вычисляют (620) вклад каждого пакета в снижение искажения изображения.

3. Способ по п.1, дополнительно содержащий этап, на котором выбирают (650) по меньшей мере одну часть пакета для защиты.

4. Способ по п.1, дополнительно содержащий этап, на котором выводят защищенный аудиовизуальный контент и информацию о том, какие пакеты защищены.

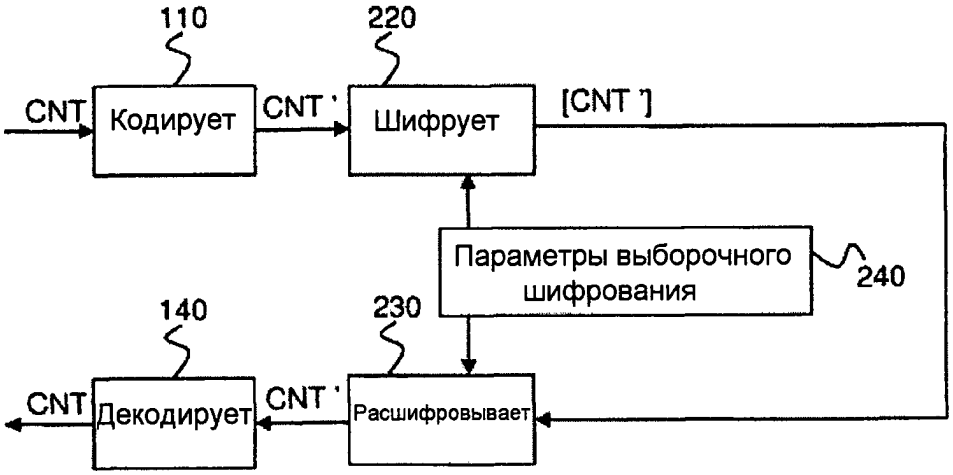
5. Способ по п.1, дополнительно содержащий этап, на котором сортируют пакеты в соответствии с их соотношением искажения к скорости передачи.

6. Устройство (800) для защиты сжатого аудиовизуального контента, организованного в набор пакетов (CNT'), содержащее устройство (820) защиты, выполненное с возможностью: вычислять соотношение искажения к скорости передачи для каждого пакета в наборе пакетов; шифровать незащищенный пакет с наибольшим соотношением искажения к скорости передачи из набора пакетов; и повторять этап шифрования только до тех пор, пока не будет получено предопределенное искажение аудиовизуального контента.



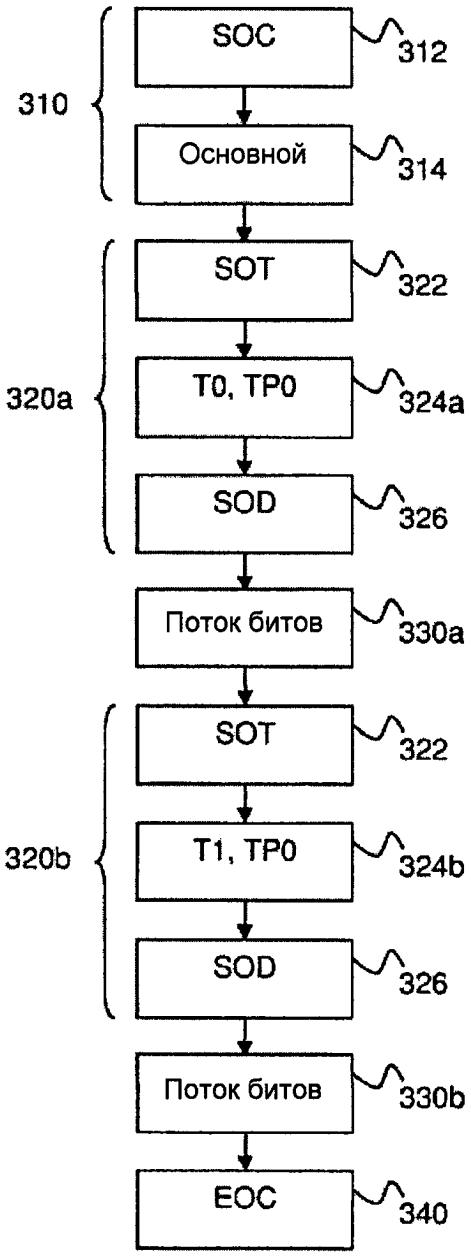
(Известный уровень техники)

ФИГ.1



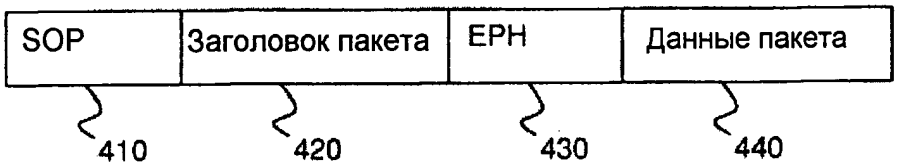
(Известный уровень техники)

ФИГ.2



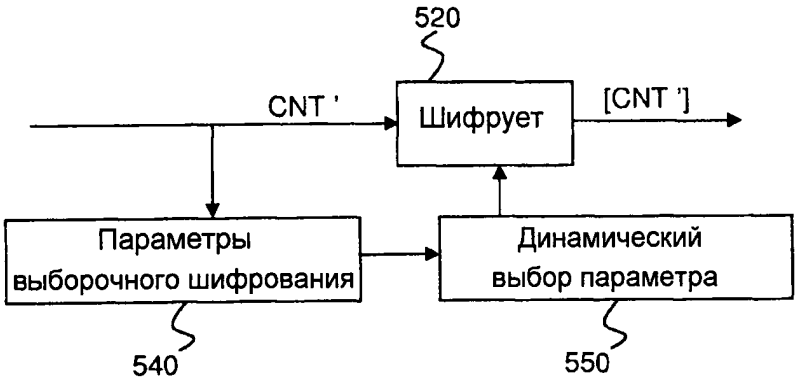
(Известный уровень техники)

ФИГ.3

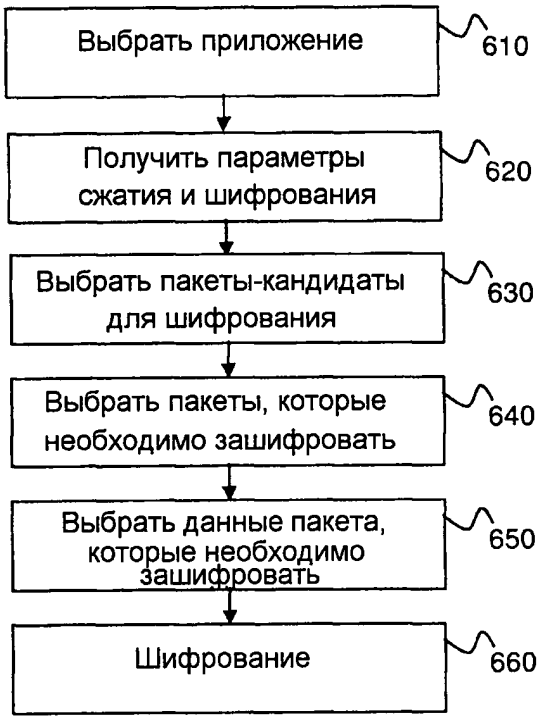


(Известный уровень техники)

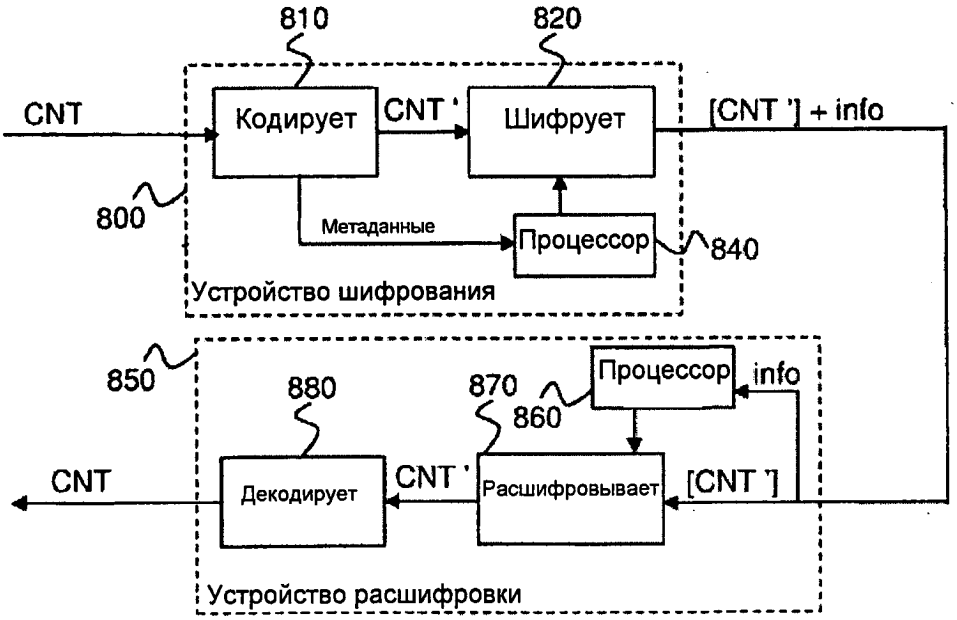
ФИГ.4


520
CNT '
Шифрует
[CNT ']
Параметры выборочного шифрования
Динамический выбор параметра
540
550

ФИГ.5


Выбрать приложение
610
Получить параметры сжатия и шифрования
620
Выбрать пакеты-кандидаты для шифрования
630
Выбрать пакеты, которые необходимо зашифровать
640
Выбрать данные пакета, которые необходимо зашифровать
650
Шифрование
660

ФИГ.6


810
820
CNT
Кодирует
CNT '
Шифрует
[CNT '] + info
800
Метаданные
Процессор
840
Устройство шифрования
850
880
870
860
Процессор
info
CNT
Декодирует
CNT '
Расшифровывает
[CNT ']
Устройство расшифровки

ФИГ.8