



ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ,
ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ

(12) **ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ**

(21), (22) Заявка: 2001113515/28, 11.10.1999

(24) Дата начала отсчета срока действия патента:
11.10.1999

(30) Конвенционный приоритет:
19.10.1998 FR 98/13074

(43) Дата публикации заявки: 10.06.2003

(45) Опубликовано: 20.01.2007 Бюл. № 2

(56) Список документов, цитированных в отчете о
поиске: EP 0773490 A, 14.05.1997. EP 0785547
A, 23.07.1997. JP 60193143 A, 01.10.1985. RU
96105402, 20.06.1998.

(85) Дата перевода заявки РСТ на национальную фазу:
21.05.2001

(86) Заявка РСТ:
FR 99/02425 (11.10.1999)

(87) Публикация РСТ:
WO 00/23993 (27.04.2000)

Адрес для переписки:
103735, Москва, ул. Ильинка, 5/2, ООО
"Союзпатент", пат.пов. С.Б.Фелицыной, рег. №
303

(72) Автор(ы):
ФЮРОН Тедди (FR),
ШЕВРО Сильвен (FR),
ДИЕЛЬ Эрик (FR)

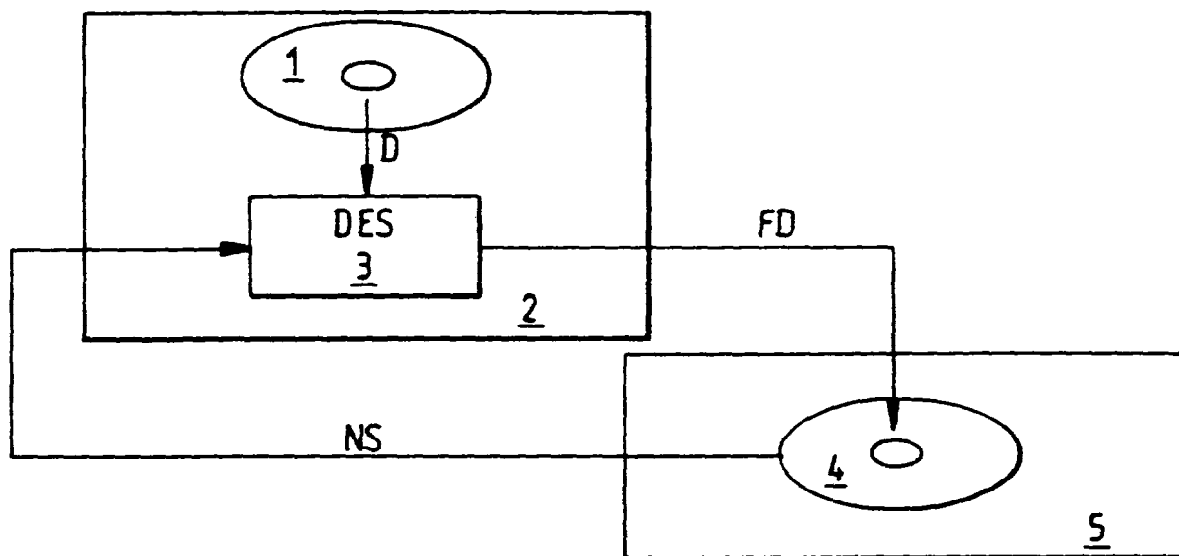
(73) Патентообладатель(и):
ТОМСОН МЮЛЬТИМЕДИА (FR)

(54) **СПОСОБ КОПИРОВАНИЯ, УСТРАНЯЮЩИЙ ВОЗМОЖНОСТЬ ПОБИТНОГО КОПИРОВАНИЯ
ЦИФРОВЫХ ДАННЫХ, И СЧИТЫВАЮЩЕЕ УСТРОЙСТВО ДЛЯ ЕГО ОСУЩЕСТВЛЕНИЯ**

(57) Реферат:

Настоящее изобретение относится к способу копирования, который предотвращает побитное копирование цифровых данных, представляющих аудио и/или видео содержание, а также к считывающему устройству, предназначенному для осуществления этого способа. В соответствии с этим способом носитель записи, на который должны быть скопированы цифровые данные,

содержит порядковый номер, используемый для форматирования считываемых цифровых данных перед записью их на указанный носитель записи. Настоящее изобретение относится, в частности, к копированию DVD, CD, магнитных лент или подобных носителей данных. Технический результат - предотвращение неразрешенного копирования цифровых данных. 4 н. и 7 з.п. ф-лы, 1 ил.





FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY,
PATENTS AND TRADEMARKS

(12) ABSTRACT OF INVENTION

(21), (22) Application: 2001113515/28, 11.10.1999

(24) Effective date for property rights: 11.10.1999

(30) Priority:
19.10.1998 FR 98/13074

(43) Application published: 10.06.2003

(45) Date of publication: 20.01.2007 Bull. 2

(85) Commencement of national phase: 21.05.2001

(86) PCT application:
FR 99/02425 (11.10.1999)

(87) PCT publication:
WO 00/23993 (27.04.2000)

Mail address:
103735, Moskva, ul. Il'inka, 5/2, OOO
"Sojuzpatent", pat.pov. S.B.Felitsynoj, reg. № 303

(72) Inventor(s):

FJuRON Teddi (FR),
ShEVRO Sil'ven (FR),
DIEL' Ehrik (FR)

(73) Proprietor(s):

TOMSON MJuL'TIMEDIA (FR)

(54) METHOD OF COPYING, WHICH REMOVES THE ABILITY OF BITWISE COPYING OF DIGITAL DATA, AND READING DEVICE FOR ITS IMPLEMENTATION

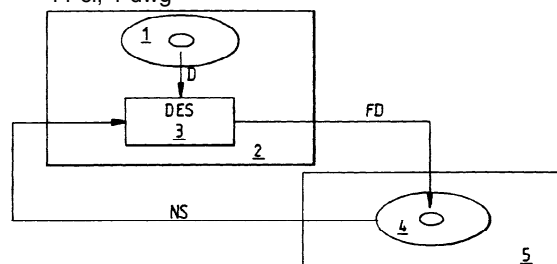
(57) Abstract:

FIELD: copying method, which removes the ability of bitwise copying of digital data, which represent audio and/or video content; reading device that implement this method; DVD, CD and magnetic tape copying.

SUBSTANCE: medium, which is used to hold the copied digital data, has a serial number, which is used for formatting the read digital data before recording them to the defined record-holding medium.

EFFECT: prevention of forbidden digital data copying.

11 cl, 1 dwg



Настоящее изобретение относится к способу копирования, который устраняет возможность побитного копирования цифровых данных, поступающих из первого источника на носитель записи. Оно также относится к устройству, используемому для осуществления этого способа.

5 Цифровые данные могут быть скопированы без существенной потери их качества. Действительно, копирование состоит в передаче последовательности двоичной информации, а именно "1" и "0", от источника данных в устройство записи. Ошибки, которые обычно происходят во время копирования, легко исправляются с использованием хорошо известных способов исправления ошибок. При этом, когда носитель данных или
10 источник информации содержат цифровые данные, можно относительно просто записывать их идентично на носитель, предназначенный для записи.

Для защиты цифровых данных от запрещенного копирования используются различные способы.

Обычно поставщик снабжает цифровой носитель данных, такой как дискета, меткой, предотвращающей какое-либо копирование данных, когда они представляют собой
15 программное обеспечение.

В документе EP-A-0773490 предложена система, предназначенная для защиты информации, записанной на носитель записи, причем в этой системе каждый носитель содержит определенный идентификатор.

20 Другой способ защиты цифровых данных от копирования состоит в снабжении их водяным знаком или "татуировкой", которые представляют собой дополнительные данные, связанные с цифровыми данными. Водяной знак не должен иметь возможность модифицирования или стирания. В данном случае считывание данных выполняется с помощью частного ключа, который идентифицирует водяной знак. В случае необходимости
25 выполнения какого-либо копирования цифровых данных с водяным знаком требуется применение частного ключа для установки водяного знака обратно на место на копии, без которого копия становится незаконной, поскольку на ней не будет водяного знака. Цифровые данные, скопированные без водяного знака, больше не считываются считывающим устройством, так как последнее не идентифицирует водяной знак там, где
30 оно должно его найти. Таким образом, водяной знак предотвращает возможность копирования без использования частного ключа.

Эти известные способы защиты от копирования обычно являются эффективными, когда носитель записи обрабатывается с помощью соответствующих устройств считывания или записи. Однако эти способы не позволяют предотвратить пиратское копирование, когда
35 создается дубль или клон, который является аналогичным, насколько это возможно, оригиналу с выполнением так называемого побитного копирования.

Настоящее изобретение направлено на способ копирования, который предотвращает неразрешенное копирование цифровых данных, поступающих из первого источника на носитель записи, причем этот способ предотвращает возможность побитного копирования
40 цифровой информации.

Целью настоящего изобретения также является считывающее устройство, содержащее схемы, осуществляющие воплощение данного способа.

В соответствии с этим предметом настоящего изобретения является способ копирования, который устраняет возможность побитного копирования цифровых данных, поступающих из источника цифровых данных на носитель записи. В соответствии с
45 настоящим изобретением способ содержит этап форматирования цифровых данных, поступающих из указанного источника цифровых данных, как функцию порядкового номера, записанного на указанный носитель и этап записи указанных отформатированных данных на указанный носитель.

50 В соответствии с предпочтительным вариантом воплощения на носителе записи во время его производства записывают порядковый номер таким образом, что его невозможно сфальсифицировать. Для предотвращения в максимальной степени вероятности пиратского копирования порядковый номер должен представлять собой уникальный номер

для каждого носителя или иметь низкую вероятность повторения для двух носителей записи.

Кроме того, форматирование цифровых данных, которые должны копироваться, выполняется с использованием алгоритма с секретным ключом, такого как DES (Стандарт шифрования данных), или алгоритма шифрования открытым ключом (доступным группе пользователей), такого как RSA, причем этот ключ зависит от порядкового номера.

Предпочтительно ключ кодирования дополнительно зависит от секретного параметра, который содержится в любом считывающем устройстве, приспособленном для считывания цифровых данных, поступающих от указанного источника данных.

Настоящее изобретение также относится к способу копирования, который устраняет возможность побитного копирования цифровых данных, считываемых устройством считывания и копируемых на носитель записи, согласно изобретению этот носитель записи содержит порядковый номер, и тем, что способ копирования содержит следующие этапы:

- передача порядкового номера, записанного на носитель записи в считывающее

устройство,

- форматирование считанных цифровых данных с помощью порядкового номера,
- запись на указанный носитель записи отформатированных цифровых данных.

В соответствии с предпочтительным вариантом воплощения этап форматирования выполняется в считывающем устройстве. Указанное считывающее устройство, кроме того, содержит средство, позволяющее производить считывание с носителя записи, содержащего отформатированные цифровые данные.

В соответствии с дополнительной характеристикой способа в соответствии с настоящим изобретением перед выполнением копирования цифровых данных способ содержит этап проверки авторизации копирования.

Настоящее изобретение также относится к считывающему устройству, позволяющему выполнить воплощение указанных способов копирования, описанных выше. В соответствии с этим аспектом настоящего изобретения устройство содержит схему форматирования, приспособленную для приема порядкового номера носителя записи, на который должны быть записаны цифровые данные, и подающую на выход отформатированные данные, которые зависят от указанного порядкового номера и предназначены для копирования на указанный носитель записи.

Настоящее изобретение также относится, в соответствии с другим аспектом, к носителю записи цифровых данных, содержащему порядковый номер, который является уникальным или имеет малую вероятность совпадения с другим носителем записи, согласно изобретению он дополнительно содержит записанные цифровые данные, причем указанные цифровые данные являются отформатированными в функции от указанного порядкового номера и от секретного параметра.

Другие характеристики и преимущества настоящего изобретения станут очевидными из нижеследующего описания предпочтительного варианта воплощения, которое приведено со ссылкой на чертеж:

чертеж изображает блок-схему считывающего устройства и устройства записи, которые позволяют выполнять копирование информации с первого носителя записи на второй носитель записи.

Настоящее изобретение будет описано со ссылкой на считывание цифровых данных, записанных на цифровой носитель записи, такой как DVD, что обозначает Универсальный цифровой диск, и копируемых на второй чистый носитель записи, который также представляет собой DVD, который в данном случае должен иметь возможность записи, а именно DVD-R. Однако для специалистов в данной области техники очевидно, что могут использоваться другие источники цифровой информации, в частности цифровая информация, получаемая с декодера и посылаемая "широковещательным передающим устройством" или цифровая информация, записанная на носитель записи, такой как магнитная лента, оптический диск с возможностью записи или без возможности записи, а именно CD, CD-R, CD-RW, DVD, DVD-R, магнитооптический диск или тому подобные.

Носитель записи состоит из магнитной ленты с возможностью записи, CD-R, CD-RW, DVD-R или магнитооптического диска, позволяющего производить накопление аудио- и/или видеoinформации в цифровой форме.

Как представлено чертеже, способ копирования в соответствии с настоящим

5 изобретением позволяет копировать цифровую информацию D, записанную на DVD 1, с использованием считывающего устройства 2, которое имеет схему 3 форматирования, и данные FD, которые могут быть скопированы, записываются на DVD-R 4, который установлен в устройство 5 записи.

10 В соответствии с настоящим изобретением DVD-R 4, который представляет собой чистый DVD-R, содержит порядковый номер, который записан во время производства DVD-R так, что его невозможно сфальсифицировать, Этот порядковый номер, который выбирается таким образом, что он является уникальным или имеет очень низкую вероятность повторения на двух различных носителях записи, записывается в скрытой области диска, такой как область, обозначаемая как "начальная дорожка", то есть

15 вступительная дорожка. Как более подробно описано ниже, этот порядковый номер используется для форматирования цифровых данных, считываемых с оригинального DVD 1.

В соответствии со способом согласно настоящему изобретению данные, считываемые с DVD 1 с помощью считывающего устройства 2, пересылаются в схему 3 форматирования, которая выполняет форматирование данных с использованием порядкового номера, считываемого с чистого DVD-R. При этом на выходе считывающего устройства получаются

20 данные FD, сформатированные определенным образом, и посылаются в устройство 5 записи, где они записываются на DVD-R 4.

Для выполнения форматирования данных так, чтобы данные, записанные на DVD-R, нельзя было скопировать побитно, но которые могли бы, однако, считываться

25 последовательно с помощью считывающего устройства, а именно для выполнения так называемой законной копии, могут использоваться различные способы форматирования. Один из обычных процессов форматирования представляет собой алгоритм кодирования с секретным ключом, такой как алгоритм DES, что обозначает "Стандарт шифрования данных" (Data Encryption Standard), который хорошо известен специалистам в данной области техники. Для предотвращения какого-либо пиратского копирования используется

30 ключ, в данном случае ключ, который строится с помощью секретного ключа и порядкового номера, считываемого с чистого DVD-R. Для выполнения форматирования с использованием этого алгоритма данные, записанные на оригинальном DVD, разбиваются на блоки по 64 бита, затем формируются с помощью DES с использованием 56-битового

35 ключа, полученного из порядковых номеров. На выходе получаются 64-битовые форматированные или зашифрованные пакеты данных, и они записываются с помощью устройства 5 записи на DVD-R 4. Если эти ключи состоят из самого порядкового номера, порядковый номер будет содержать 56 бит. Однако количество бит порядкового номера приведено только для примера. Действительно, возможно использовать настоящее

40 изобретение с носителем записи, порядковый номер которого имеет большую или меньшую длину чем 56 бит. В данном случае может применяться усечение или кодирование канала так, чтобы эти порядковые номера имели правильную длину. Если ключ представляет собой, по причинам безопасности, функцию порядкового номера, он может быть получен

45 следующим образом:

предположим, что NS представляет собой порядковый номер носителя записи, и PS представляет собой параметр, записанный секретным образом в соответствующих считывающих устройствах:

- производится конкатенация (сцепление) NS и PS так, что получается слово (NS/PS),
- 50 - применяется хэш-функция, такая как функции SHA-1 (стандарт Национального Института Стандартов и Технологий), и это приводит к получению слова SHA (NS/PS), которое имеет длину 64 бита,
- производится усечение этого слова так, что оставляется слово из 56 бит, которое

служит в качестве ключа для DES.

Длина двоичных слов NS и PS не является фиксированной, поскольку для SHA-1 точная длина входного слова не установлена. Функция f позволяет применять любую длину порядкового номера.

- 5 DVD-R 4, скопированный, таким образом, законным путем, может читаться с помощью считывающего устройства 2, и первоначальные цифровые данные восстанавливаются с использованием соответствующего алгоритма декодирования.

- Также возможно выполнять форматирование цифровых данных, которые необходимо копировать, с использованием алгоритма шифрования открытым ключом, такого как
10 алгоритм RSA. Этот алгоритм шифрования открытым ключом представляет собой асимметричный алгоритм, который, когда открытый ключ известен, предотвращает простое копирование отформатированных данных во время их считывания с помощью считывающего устройства 2.

- Поскольку данные, размещенные на копии DVD-R, не имеют такую же структуру, как и
15 данные оригинального DVD, поэтому становится невозможным восстановить их с помощью считывающего устройства, кроме как с использованием соответствующего считывающего устройства. Кроме того, если была сделана побитная копия оригинального DVD, считывающее устройство в соответствии с настоящим изобретением не позволит воспроизвести оригинальную цифровую информацию и не будет считывать эту копию.

- 20 В соответствии с дополнительной характеристикой настоящего изобретения перед способом копирования может выполняться этап проверки авторизации на копирование такой, как описан в заявке на французский патент №9811860, поданной 23 сентября 1998 г. на имя компании Томсон мультимедиа (THOMSON multimedia), под названием "Protection contre la copie de données numériques stockées sur un support d'information" [Защита от
25 копирования цифровых данных, записанных на носителе информации]. Эта проверка авторизации на копирование применяется к носителю записи информации, содержит первую идентификацию шифра цифровых данных, вторую идентификацию водяного знака цифровых данных, первое определение первой метки, если было возможно идентифицировать шифр и водяной знак, третью идентификацию типа носителя записи
30 данных, второе определение второй метки, если было возможно определить первую метку и если было возможно идентифицировать определенный тип носителя записи информации, четвертую идентификацию криптографических данных сигнатуры, сопровождающих цифровые данные, третье определение третьей метки, если было возможно определить вторую метку и если было возможно идентифицировать криптографические данные
35 сигнатуры и первую выдачу разрешения на цифровое копирование цифровых данных, если было возможно определить третью метку.

Все характеристики, описанные в этой заявке на французский патент, приводятся в качестве ссылки в настоящей заявке на патент для выполнения проверки авторизации копирования.

- 40 В соответствии с настоящим изобретением считывающее устройство 2, предназначенное для считывания цифровых данных, которое может представлять собой считывающее устройство DVD, декодер, считывающее устройство CD или тому подобное, содержит схему 3 форматирования, состоящую, по существу, из интегральной микросхемы, включающей все средства, необходимые для выполнения алгоритма, выбранного для
45 форматирования и осуществления возможности записи с невозможностью фальсификации определенных данных, таких как секретный ключ или средство для авторизации копирования.

Вариант воплощения, описанный выше, приведен в качестве примера и может быть модифицирован без выхода из рамок прилагаемой формулы изобретения.

50

Формула изобретения

1. Способ копирования цифровых данных, представляющих аудио- и/или видеосодержание, поступающих с источника цифровых данных (1) на накопитель (4),

отличающийся тем, что указанный способ содержит следующие этапы: форматирование цифровых данных, поступающих от указанного источника цифровых данных, как функция порядкового номера (NS), находящегося на указанном носителе (4) для получения данных, форматированных специально для указанного носителя, и для устранения возможности побитного копирования цифровых данных на другой накопитель, при этом порядковый номер (NS) представляет собой уникальный номер для каждого носителя записи или имеет низкую вероятность совпадения для двух носителей записи, и запись указанных форматированных данных (FD) на указанный носитель.

2. Способ по п.1, отличающийся тем, что порядковый номер (NS) записан на носителе (4) во время его производства так, что его невозможно сфальсифицировать.

3. Способ по любому одному из пп.1 и 2, отличающийся тем, что этап форматирования цифровых данных, которые необходимо копировать, выполняется с использованием алгоритма кодирования с использованием секретного ключа, такого, как DES или алгоритм шифрования открытым ключом такой, как RSA.

4. Способ по п.3, отличающийся тем, что ключ кодирования зависит от порядкового номера (NS).

5. Способ по п.4, отличающийся тем, что ключ кодирования дополнительно зависит от секретного параметра (PS), содержащегося на любом считывающем устройстве (2), которое приспособлено для считывания цифровых данных, поступающих с указанного источника.

6. Способ копирования цифровых данных, представляющих аудио- и/или видеосодержание, считываемых с помощью считывающего устройства (2) и копируемых на носитель (4), отличающийся тем, что носитель содержит порядковый номер (NS), при этом порядковый номер (NS) представляет собой уникальный номер для каждого носителя записи или имеет низкую вероятность совпадения для двух носителей записи, и что способ копирования содержит этапы

передача порядкового номера (NS), записанного на носителе (4), на считывающее устройство (2),

форматирование считанных цифровых данных с помощью порядкового номера для получения данных, форматированных специально для указанного носителя, и запись указанных форматированных данных на указанный носитель (4).

7. Способ по п.6, отличающийся тем, что этап форматирования выполняется в считывающем устройстве (2).

8. Способ по любому из п.6 или 7, отличающийся тем, что считывающее устройство (2) содержит средство, позволяющее производить считывание с носителя, содержащего отформатированные цифровые данные.

9. Способ по любому одному из пп.6-8, отличающийся тем, что перед выполнением копирования цифровых данных он содержит этап проверки авторизации на копирование.

10. Считывающее устройство (2), предназначенное для считывания цифровых данных, представляющих аудио- и/или видеосодержание, и для форматирования указанных цифровых данных, записываемых на носитель, отличающееся тем, что оно содержит схему (3) форматирования, приспособленную для приема порядкового номера (NS) с носителя, при этом порядковый номер (NS) представляет собой уникальный номер для каждого носителя записи или имеет низкую вероятность совпадения для двух носителей записи, и считывающее устройство выполнено с возможностью формирования выходных данных (FD), форматированных специально для указанного носителя, которые зависят от указанного порядкового номера (NS), и которые предназначены для копирования на указанный носитель записи.

11. Носитель (4) записи для цифровых данных, представляющих аудио и/или видео содержание, содержащий порядковый номер (NS), который является уникальным или имеет низкую вероятность повторения на другом носителе записи, отличающийся тем, что он дополнительно содержит записанные цифровые данные (FD), причем указанные цифровые данные (FD) отформатированы специально для указанного носителя, как

функция указанного порядкового номера (NS) и секретного параметра (PS).

5

10

15

20

25

30

35

40

45

50