РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

(19) **RU** (11) **2 673 620**(13) **C2**

(51) МПК
B41J 2/175 (2006.01)

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ПАТЕНТУ

(52) СПК
B41J 2/175 (2006.01)

(21)(22) Заявка: **2017114375, 31.10.2014**

(24) Дата начала отсчета срока действия патента:
31.10.2014

Дата регистрации:
28.11.2018

Приоритет(ы):
(22) Дата подачи заявки: **31.10.2014**

(43) Дата публикации заявки: **25.10.2018** Бюл. № **30**

(45) Опубликовано: **28.11.2018** Бюл. № **34**

(85) Дата начала рассмотрения заявки PCT на национальной фазе: **25.04.2017**

(86) Заявка PCT:
US 2014/063381 (31.10.2014)

(87) Публикация заявки PCT:
WO 2016/068990 (06.05.2016)

Адрес для переписки:
129090, Москва, ул. Большая Спасская, д. 25, строение 3, ООО "Юридическая фирма Городисский и Партнеры"

(72) Автор(ы):
НЭСС Эрик Д. (US),
РАЙС Хастон У. (US),
ХОЛЛ Брендан (IE)

(73) Патентообладатель(и):
ХЬЮЛЕТТ-ПАККАРД ДИВЕЛОПМЕНТ КОМПАНИ, Л.П. (US)

(56) Список документов, цитированных в отчете о поиске: **US 20060050103 A1, 09.03.2006. US 20090225609 A1, 10.09.2009. US 20030146951 A1, 07.08.2003. JP 2009300758 A, 24.12.2009. US 20030184624 A1, 02.10.2003.**

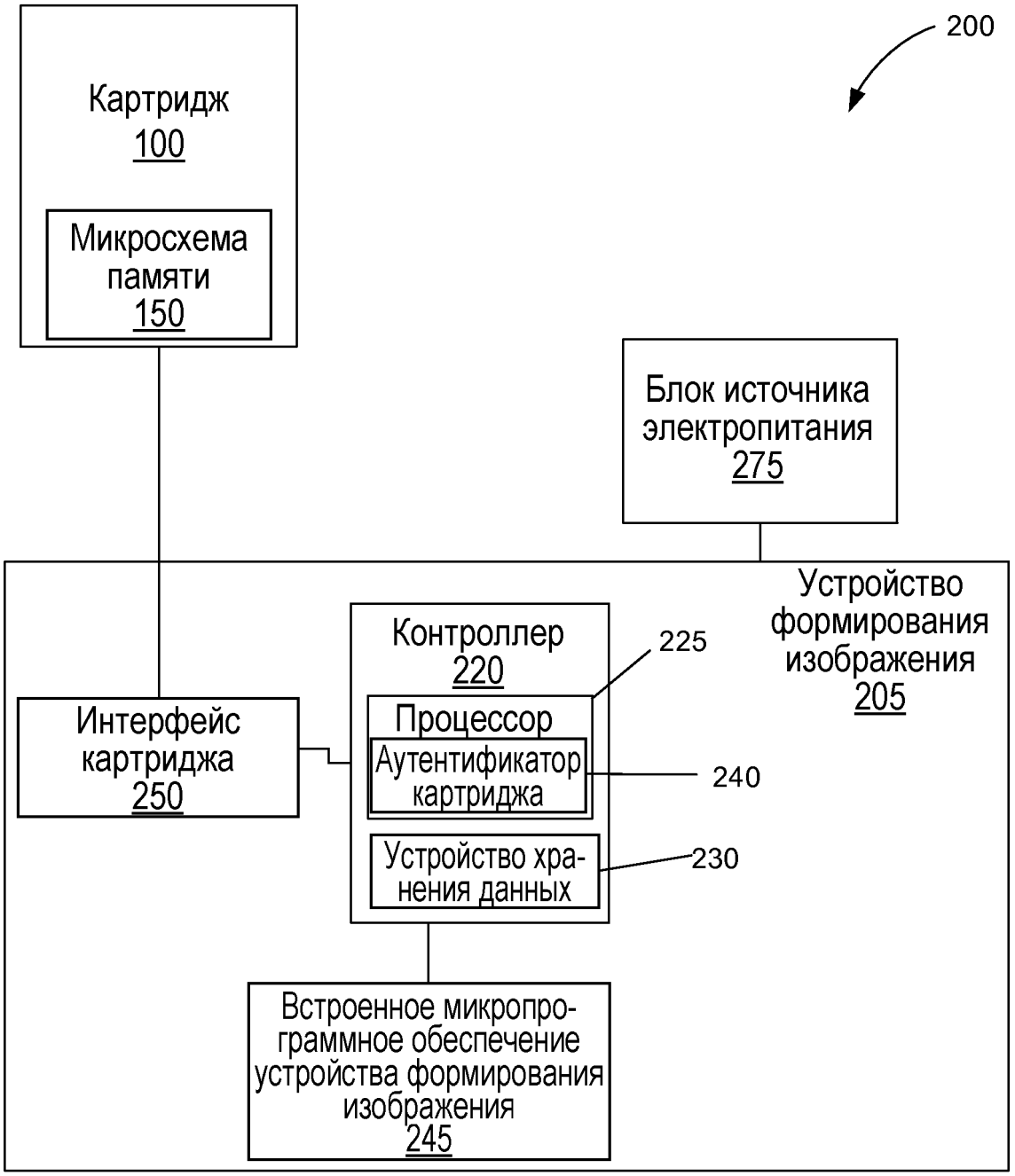
(54) ШИФРОВАНИЕ КАРТРИДЖЕЙ С ТЕКУЧЕЙ СРЕДОЙ ДЛЯ ИСПОЛЬЗОВАНИЯ В УСТРОЙСТВАХ ФОРМИРОВАНИЯ ИЗОБРАЖЕНИЯ

(57) Реферат:

Раскрывается шифрование картриджей с текучей средой для использования в устройствах формирования изображения. Одно из раскрытых устройств содержит память картриджа с текучей средой, содержащую множество последовательных битов, причем множество последовательных битов записывается после того, как множество последовательных битов преобразуется, основываясь на скремблирующих битах из множества последовательных битов, и интерфейс памяти картриджа с текучей средой для разрешения доступа к памяти, чтобы аутентифицировать картридж с текучей средой. 3 н. и 11 з.п. ф-лы, 7 ил.

RU 2673620 C2

RU 2673620 C2



ФИГ. 2

RU 2673620 C2

RU 2673620 C2

RUSSIAN FEDERATION

FEDERAL SERVICE
FOR INTELLECTUAL PROPERTY

(19) **RU** (11) **2 673 620**(13) **C2**

(51) Int. Cl.
B41J 2/175 (2006.01)

(12) ABSTRACT OF INVENTION

(52) CPC
B41J 2/175 (2006.01)

(21)(22) Application: **2017114375, 31.10.2014**

(24) Effective date for property rights:
31.10.2014

Registration date:
28.11.2018

Priority:
(22) Date of filing: **31.10.2014**

(43) Application published: **25.10.2018** Bull. № **30**

(45) Date of publication: **28.11.2018** Bull. № **34**

(85) Commencement of national phase: **25.04.2017**

(86) PCT application:
US 2014/063381 (31.10.2014)

(87) PCT publication:
WO 2016/068990 (06.05.2016)

Mail address:
129090, Moskva, ul. Bolshaya Spasskaya, d. 25, stroenie 3, OOO "Yuridicheskaya firma Gorodisskij i Partnery"

(72) Inventor(s):
NESS Erik D. (US),
RICE Huston W. (US),
HALL Brendan (IE)

(73) Proprietor(s):
HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (US)

RU 2673620 C2

RU 2673620 C2

(54) ENCRYPTION OF FLUID CARTRIDGES FOR USE WITH IMAGING DEVICES

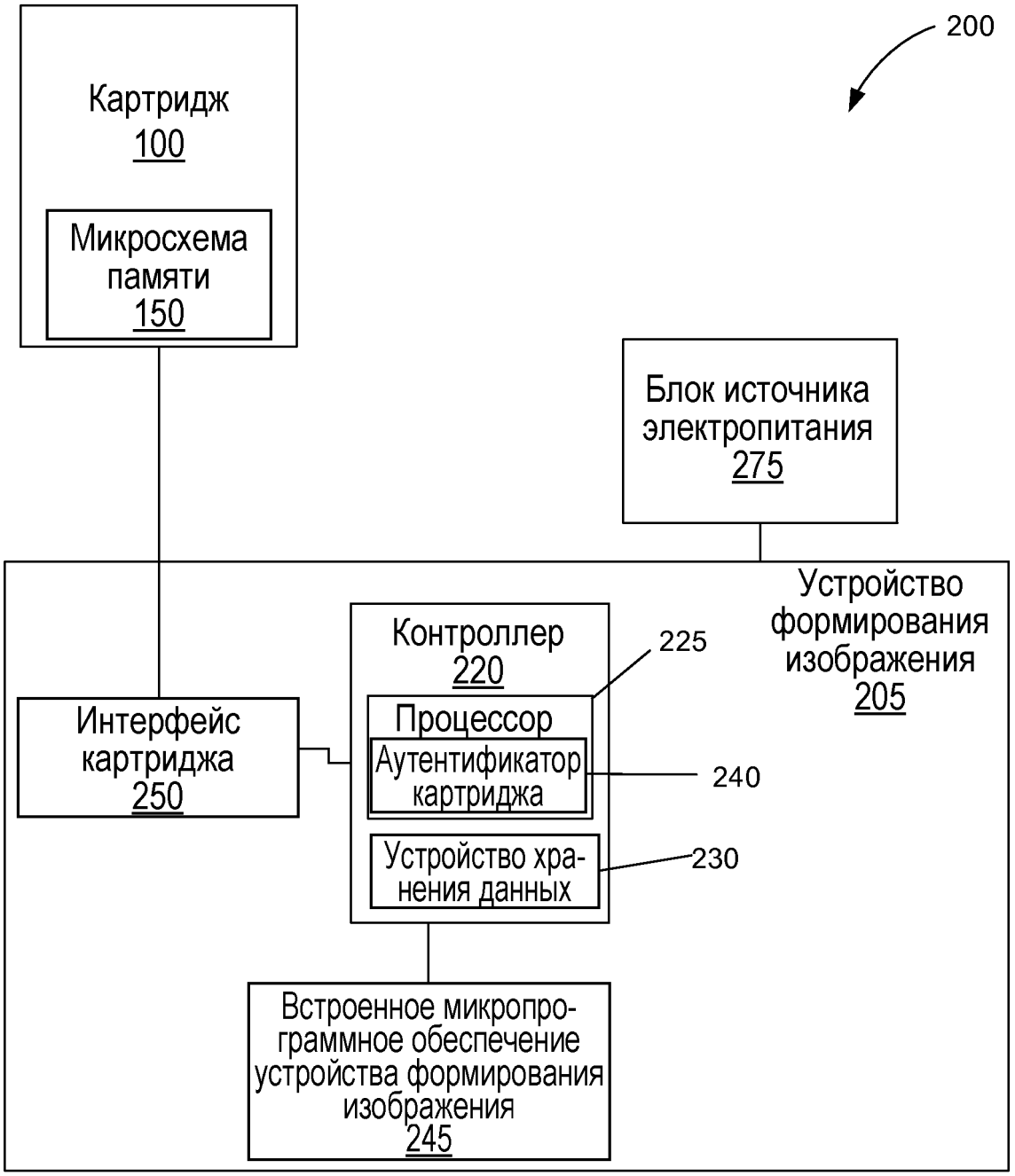
(57) Abstract:

FIELD: image forming devices.

SUBSTANCE: one of the disclosed devices comprises a fluid cartridge memory comprising a plurality of sequential bits, wherein the plurality of sequential bits is recorded after the plurality of sequential bits are converted, based on the scrambling bits of the plurality of sequential bits, and the fluid cartridge memory interface for enabling memory access to authenticate the fluid cartridge.

EFFECT: disclosed is encryption of fluid cartridges for use in imaging devices.

14 cl, 7 dwg



ФИГ. 2

RU 2673620 C2

RU 2673620 C2

Уровень техники

Устройства формирования изображения на основе чернил используют чернила для печати изображений на носителе. Обычно, чернила, содержащиеся в картриджах с текучей средой (например, в картриджах с чернилами, картриджах), со временем заканчиваются и картриджи, в конечном счете, должны заменяться, чтобы продолжать работу устройства формирования изображения. Установка или замена картриджа в устройстве формирования изображения (например, в принтере, сканере, копире и т. д.) перед использованием в устройстве формирования изображения иногда требует аутентификации и/или проверки подлинности. В некоторых ситуациях предпочтительно иметь надежную аутентификацию и/или проверку подлинности устройства, чтобы проверить подлинность картриджа в неконтролируемой среде (например, в среде потребителя).

Краткое описание чертежей

Фиг. 1 - примерный картридж с текучей средой, в котором могут быть реализованы раскрытые в данном документе примеры.

Фиг. 2 - схематичное представление системы аутентификации картриджа, соответствующей принципам настоящего раскрытия.

Фиг. 3 - схематичное представление примерной реализации примерного аутентификатора картриджа устройства формирования изображения в системе аутентификации картриджа, показанной на фиг. 2.

Фиг. 4 - пример битовой матрицы, которой манипулируют на этапах шифрования последовательности битов и которая может использоваться в раскрытых в данном документе примерах.

Фиг. 5 - блок-схема последовательности операций, представляющая примерные машиночитаемые команды, которые могут исполняться для реализации примерной системы аутентификации картриджа, показанной на фиг. 2.

Фиг. 6 - другая блок-схема последовательности операций, представляющая примерные машиночитаемые команды, которые могут исполняться для реализации примерного картриджа примерной системы аутентификации картриджа, показанной на фиг. 2.

Фиг. 7 - блок-схема примерной платформы процессора, способной исполнять примерные машиночитаемые команды, показанные на фиг. 5 и 6.

Чертежи приведены не в масштабе. Везде, где возможно, одни и те же ссылочные позиции будут использоваться на всех чертежах и в сопроводительном письменном описании для ссылки на одни и те же или схожие части.

Подробное описание

В данном документе раскрывается шифрование картриджей с текучей средой для использования в устройствах формирования изображения. Обычно картриджи с текучей средой (например, картриджи с чернилами, картриджи и т. д.) для использования с устройствами формирования изображения (например, с принтерами, сканерами, копирами и т. д.) требуют замены из-за окончания чернил, содержащихся в картриджах с текучей средой. Некоторые известные картриджи имеют постоянную память с битовой последовательностью для проверки подлинности таких картриджей, выполняемой устройствами формирования изображения. В этих известных примерах вся битовая последовательность или участок битовой последовательности картриджа проверяется на наличие допустимых значений относительно заданных устройством формирования изображения критериев авторизации картриджей. Чтобы провести реинжиниринг этих картриджей, третьи лица могут сделать выборку множества картриджей, чтобы определить, какие адреса или участки битовой последовательности совместимы у

множества картриджей, выбранных для создания неавторизованных картриджей.

Раскрытые в данном документе примеры представляют технологию шифрования и/или дешифрования для предотвращения реинжиниринга картриджей, чтобы не допустить использование и/или распространение неавторизованных картриджей. В частности, раскрытые в данном документе примеры преобразуют множество последовательных битов (например, битовую последовательность, множество битов и т. д.), соответствующих памяти картриджа (например, скопированных или которые должны быть записаны в блок памяти), основываясь на скремблирующих битах из множества последовательных битов. В некоторых примерах скремблирующие биты являются битами с заданными или известными адресами из множества последовательных битов, используемых для определения, как сдвинуть или перегруппировать нестатические биты (например, биты, разрешенные для перегруппирования, преобразования, сдвинуть и т. д.) из множества последовательных битов. В некоторых примерах статические биты из множества последовательных битов остаются теми же самыми и не перемещаются, не сдвигаются и/или не меняют последовательность. В некоторых примерах статические биты и/или участок статических битов определяют скремблирующие биты. Раскрытые здесь примеры могут использоваться в сочетании с другими способами обеспечения безопасности, проверки подлинности и/или шифрования для предотвращения реинжиниринга картриджей.

Раскрытые в данном документе примеры позволяют программировать память аутентификации картриджа, определяя скремблирующие биты из множества последовательных битов для памяти аутентификации картриджа, преобразовывать, используя процессор, множество последовательных битов, основываясь на скремблирующих битах, и сохранять преобразованное множество последовательных битов в памяти аутентификации. В некоторых примерах преобразование множества последовательных битов содержит сдвиг нестатических битов из множества последовательных битов, основываясь на скремблирующих битах. В некоторых примерах скремблирующие биты исключаются из преобразования. В некоторых примерах скремблирующие биты находятся в заданных ячейках памяти аутентификации. В некоторых примерах преобразование множества последовательных битов основывается на алгоритме, определенном по скремблирующим битам.

Термин "преобразование" или "перемещение", как он используется в данном документе со ссылкой на бит и/или битовую последовательность, может относиться к перемещению и/или сдвигу бита в памяти или к перемещению бита копии битовой последовательности в оперативной памяти (RAM). Битовая последовательность может копироваться или приниматься из постоянной памяти (ROM) или из стираемой программируемой постоянной памяти (EPROM, устройство EPROM и т.д.), например, устройства формирования изображения. "Перемещение" или "сдвиг" могут также относиться к копированию бита или битовой последовательности из одного адресной ячейки или адресной ячейки матрицы в другую адресную ячейку матрицы. Термин "рекурсивно", как он используется в данном документе, относится, к перемещению между концами битовой последовательности. Например, бит, сдвинутый или перемещенный из ячейки на конце или вблизи конца одномерной матрицы (например, битовой последовательности) может перемещаться в начало одномерной матрицы и так далее.

На фиг. 1 представлен примерный картридж 100 с текучей средой (например, картридж для чернил, картридж для печати и т. д..) 100, в виде которого могут быть реализованы раскрытые здесь примеры. Примерный картридж 100 содержит резервуар

110 для текучей среды, головку 120, содержащую сопла, гибкий кабель (например, гибкую печатную плату) 130, контактные площадки 140 и микросхему 150 памяти (например, память, устройство памяти, банк памяти и т. д.). Гибкий кабель 130, показанный в примере, соединяется (например, приклеивается и/или монтируется) к боковым сторонам картриджа 100 и включает в себя дорожки и/или интерфейс памяти (например, схему интерфейса памяти и т. д.), которые электрически соединяют микросхему 150 памяти, головку 120 и контактные площадки 140. В некоторых примерах микросхема 150 памяти и/или функциональные устройства, связанные с микросхемой 150 памяти, интегрируются с головкой 120 и/или со сборочным узлом печатной схемы головки.

Микросхема 150 памяти, показанная на примере, содержит битовую последовательность аутентификации. В данном примере, микросхема 150 памяти может также содержать множество другой информации, в том числе, тип картриджа, тип текучей среды, содержащейся в картридже, оценку количества текучей среды в картридже 110 для текучей среды, дату калибровки, информацию об ошибках, информацию об обслуживании и/или другие данные.

На фиг. 2 схематично представлена система 200 аутентификации картриджа в соответствии с принципами настоящего раскрытия. В этом примере система 200 аутентификации картриджа имеет устройство 205 формирования изображения (например, принтер), коммуникативно соединенное с картриджем 100, описанным выше на фиг. 1. Устройство 205 формирования изображения, показанное на примере, содержит контроллер 220, имеющий процессор 225, устройство 230 хранения данных и аутентификатор 240 картриджа, который может быть реализован процессором 225. Устройство 205 формирования изображения также содержит встроенное микропрограммное обеспечение 245 устройства формирования изображения, которое может храниться в устройстве 230 хранения данных, и интерфейс 250 картриджа. Встроенное микропрограммное обеспечение 245 в примере, показанном на чертеже, исполняется процессором 225 и заставляет и/или инициирует процессор 225 для получения доступа к микросхеме 150 памяти картриджа 100. В этом примере блок 275 источника электропитания, соединенный с устройством 205 формирования изображения, обеспечивает электропитание как устройства 205 формирования изображения, так и картриджа 100.

При работе примерный картридж 100 устанавливается в держатель картриджа примерного устройства 205 формирования изображения. Устройство 205 формирования изображения, показанное в примере, средствами связи соединяется с картриджем 100 для аутентификации картриджа 100 и управления картриджем 100 через интерфейс 250 картриджа. Интерфейс 250 картриджа, показанный в примере, состоит из электрических контактов устройства 205 формирования изображения, входящих в контакт с проводящими площадками 140, показанными выше на фиг. 1, когда картридж 100 вставляется в держатель устройства 205 формирования изображения, чтобы позволить устройству 205 формирования изображения осуществлять связь с картриджем 100, управлять электрическими устройствами или функциями осаждения чернил картриджа 100 и/или проверять подлинность подлинности картриджа 100. Чтобы аутентифицировать картридж 100, устройство 205 формирования изображения получает доступ по адресу ячейки памяти микросхемы 150 памяти через интерфейс 250 картриджа для приема битовой последовательности аутентификации (например, матрицы, битовой матрицы и т. д.), например, от микросхемы 150 памяти. Битовая последовательность аутентификации может быть 256-битовой последовательностью или иметь любой другой

соответствующий размер (16-битовый, 1024-битовый и т. д.). В некоторых примерах битовая последовательность аутентификации может быть многомерной матрицей. В некоторых примерах вся битовая последовательность аутентификации считывается на едином этапе.

В этом примере процессор 225, основываясь на командах, подаваемых встроенным микропрограммным обеспечением 245 устройства формирования изображения, принимает битовую последовательность аутентификации от микросхемы 150 памяти через интерфейс 250 картриджа и направляет битовую последовательность аутентификации к аутентификатору 240 картриджа, который преобразует (например, сдвигает, перестраивает, скремблирует, переназначает, перемещает и т. д.), битовую последовательность аутентификации, чтобы проверить подлинность картриджа 100. В частности, аутентификатор 240 картриджа в показанном примере определяет скремблирующие биты (например, значения скремблирующих битов), получая доступ к участку(-ам) битовой последовательности аутентификации по заданным и/или известным адресам битовой последовательности. В некоторых примерах скремблирующие биты (например, значения скремблирующих битов) указывают аутентификатору 240 картриджа и/или процессору 225 множество адресных ячеек для сдвига битов битовой последовательности аутентификации. В некоторых примерах арифметическая операция, определенная посредством и/или между скремблирующими битами, указывает и/или определяет, как аутентификатор 240 должен преобразовать битовую последовательность аутентификации. В некоторых примерах аутентификатор 240 обладает заранее определенными функциями преобразования, инициируемыми конкретными значениями скремблирующих битов и/или зависимостью между значениями скремблирующих битов (например, сумма и т. д.). В частности, значения скремблирующих битов могут сравниваться с таблицей, чтобы выбрать заранее определенную функцию(-и) преобразования для преобразования битовой последовательности аутентификации. В некоторых примерах биты из битовой последовательности аутентификации определяют множество циклов преобразования, чтобы преобразовать битовую последовательность аутентификации.

В этом примере, после преобразования битовой последовательности аутентификатор 240 картриджа осуществляет верификацию преобразованной битовой последовательности. Эта верификация может осуществляться, проверяя преобразованную битовую последовательность относительно известного значения, заданных критериев, контрольной суммы, математических операций или посредством любой другой соответствующей проверки подлинности числовой последовательности. В этом примере, когда преобразованная битовая последовательность была аутентифицирована, аутентификатор 240 картриджа через интерфейс 250 картриджа подает на процессор 225 и/или интерфейс 250 картриджа сигнал разрешения использования и/или связи между контроллером 220 и картриджем 100. В некоторых примерах контроллер 220 посылает сигнал авторизации на картридж 100, чтобы разрешить использование картриджа 100 с устройством 205 формирования изображения.

На фиг.3 показано схематичное представление одной примерной реализации примерного аутентификатора 240 картриджа устройства 205 формирования изображения, показанного на фиг. 2. Аутентификатор 240 картриджа в показанном примере содержит контроллер 306 битовой последовательности, модуль 308 скремблирования битов, интерфейс 310 памяти картриджа, модуль 312 преобразования битовой последовательности и анализатор 314 преобразованной битовой последовательности. Контроллер 306 битовой последовательности в показанном

примере подает сигнал на интерфейс 310 памяти картриджа, чтобы вызвать битовую последовательность аутентификации из памяти (например, из памяти, структуры данных памяти и т. д.) картриджа (например, картриджа 100) и подать битовую последовательность аутентификации на модуль 312 преобразования битовой последовательности. В этом примере контроллер 306 битовой последовательности переключает модуль 308 битов скремблирования, чтобы предоставить данные, такие как ячейки памяти для скремблирующих битов битовой последовательности аутентификации и/или для скремблирующих битов битовой последовательности аутентификации (например, значений скремблирующих битов, преобразованных значений скремблирующих битов и т. д.), на модуль 312 преобразования битовой последовательности, чтобы позволить модулю 312 преобразования битовой последовательности преобразовать битовую последовательность аутентификации, принятую от интерфейса 310 памяти картриджа, основываясь на скремблирующих битах. В некоторых примерах преобразование битовой последовательности аутентификации дополнительно основывается на статических битах битовой последовательности аутентификации. В некоторых примерах скремблирующие биты исключаются из процесса преобразования.

После того, как модуль 312 преобразования битовой последовательности преобразовал битовую последовательность аутентификации, преобразованная битовая последовательность аутентификации подается на анализатор 314 преобразованной битовой последовательности, который проверяет подлинность преобразованной битовой последовательности аутентификации. В некоторых примерах анализатор преобразованной битовой последовательности интерпретирует команду, основываясь на проверке подлинности преобразованной битовой последовательности и/или на сравнении принятой преобразованной битовой последовательности с таблицей известных преобразованных битовых последовательностей.

На фиг. 4 показана примерная битовая матрица 400, которой манипулируют на этапах последовательности шифрования битов. Примерная битовая матрица 400 подразделяется на 4-битовые двоичные последовательности. Битовая матрица 400 в показанном примере имеет статические биты (например, поднаборы, участки, последовательности и т. д.) 402 и 404 в заданных (например, известных) адресных ячейках примерной битовой матрицы 400. В некоторых примерах статические биты 402 и 404 распределяются случайно по всей примерной битовой матрице 400. В этом примере остающиеся биты примерной битовой последовательности являются нестатичными (например, подвижными, перезаписываемыми и т. д.). В частности, примерная битовая матрица имеет последовательности нестатических битов (например, участки) 406, 408, 410, 412, 414 и 416.

В этом примере скремблирующие биты примерной битовой матрицы 400, которые могут располагаться по заданным адресам битовой матрицы 400, и/или зависимость между скремблирующими битами определяют и/или указывают способ преобразования или команды преобразования примерной битовой матрицы 400. В этом примере скремблирующие биты являются статическими битами 402 и 404, которые определяют сдвиг каждого нестатического бита двух ячеек памяти. В частности, двоичное значение суммы статического бита 402 и статического бита 404 равно значению два, которое используется, например, для определения, сколько нужно адресных ячеек, чтобы, например, сдвинуть каждый из нестатических битов примерной битовой матрицы 400. В этом примере скремблирующие биты равны статическим битам 402 и 404 и исключаются из того, чтобы их сдвигать и/или перемещать. Однако, в некоторых

примерах, по меньшей мере один из нестатических битов содержит скремблирующие биты и скремблирующие биты могут перемещаться и/или сдвигаться. Хотя в этом примере используется сумма показанных скремблирующих битов, для определения шаблона преобразования между статическими битами и/или между статическими и нестатическими битами могут использоваться более сложные операции (например, многоэтапные арифметические операции, переменные операции между различными ячейками памяти и/или адресами и т. д.).

Битовая последовательность (например, участок) 406 примерной битовой матрицы 400 близок к сдвигу двух адресных ячеек, как направляется суммой статических битов 402 и 404 и указывается стрелкой 418. Однако, поскольку статические биты 404 находятся в назначенных статических ячейках, битовая последовательность 406 не переписывает статические биты 404. Вместо этого, битовая последовательность 406 сдвигается на дополнительные два адреса, как указано стрелкой 420. Поскольку битовая последовательность 408 не имеет двух адресов памяти статических битов для перемещения обратно из битовой последовательности 408, битовая последовательность 408 перемещается как указано стрелкой 422. Аналогично, битовая последовательность 410 перемещается на две адресные ячейки, как указано стрелкой 424, и битовая последовательность 412 также перемещается, как указано стрелкой 426. В этом примере битовые последовательности 414 и 416 перемещаются на более поздние участки примерной битовой матрицы 400 (например, на два адреса памяти, как определено статическими битами 402 и 404).

Поскольку битовые последовательности (например, участки) 406, 408, 410, 412, 414 и 416 во время процесса преобразования сдвигаются в их соответствующие адреса памяти, стрелки 428 и 430 указывают битовые последовательности из более поздних участков (например, рядом или на конце битовой матрицы 400), которые представляются как "XXXX", битовой последовательности аутентификации, перемещенной (например, рекурсивно перемещенной) в адреса памяти после статических битов 402.

В некоторых примерах статические биты 402, 404 используются для передачи информации устройству формирования изображения и/или используются для производственных или операционных процессов (например, нанесения производственных кодов, таких как коды партии, порядковый номер и т. д.). Хотя пример на фиг. 4 показывает сдвиги в одном направлении, сдвиги могут происходить, например, в противоположном направлении или некоторые биты могут сдвигаться в различных направлениях относительно других битов. В некоторых примерах различные биты сдвигаются на различное количество адресных ячеек, которое может определяться скремблирующими битами, статическими битами и/или ячейками статических битов. Хотя описанные выше примеры относятся к одномерной (1D) матрице, примеры, раскрытые здесь, могут быть применены к многомерным матрицам. Дополнительно или альтернативно, скремблирующие биты могут определять сдвиг более чем в одном направлении и/или размерности многомерных матриц. В некоторых примерах преобразование и/или переупорядочивание битовой последовательности выполняется на одном этапе, который может быть выполнен, например, многопоточным процессором.

Хотя примерный способ реализации системы 200 аутентификации картриджа, показанной на фиг. 2, показан на фиг. 5 и 6, один или более элементов, процессов и/или устройств, показанных на фиг. 5 и 6, могут объединяться, разделяться, перегруппировываться, опускаться, исключаться и/или реализовываться любым другим способом. Дополнительно, примерное устройство 205 формирования изображения,

примерный контроллер 220, примерный процессор 225, примерное запоминающее устройство 230 для хранения данных, примерный аутентификатор 240 картриджа, примерное встроенное микропрограммное обеспечение 245 устройства формирования изображения, примерный интерфейс 250 картриджа, примерный картридж 100, примерная микросхема 150 памяти, примерный контроллер 306 битовой последовательности, примерный модуль 308 статических битов, примерный интерфейс 310 памяти картриджа, примерный модуль 312 преобразования битовой последовательности, примерный анализатор 314 преобразованной битовой последовательности и/или, в более широком смысле, примерная система 200 аутентификации картриджа, показанная на фиг. 2, могут осуществляться аппаратным обеспечением, программным обеспечением, встроенным микропрограммным обеспечением и/или любой комбинацией аппаратного обеспечения, программного обеспечения и/или встроенного микропрограммного обеспечения. Таким образом, например, любое примерное устройство 205 формирования изображения, примерный контроллер 220, примерный процессор 225, примерное запоминающее устройство 230 хранения данных, примерный аутентификатор 240 картриджа, примерное встроенное микропрограммное обеспечение 245 устройства формирования изображения, примерный интерфейс 250 картриджа, примерный картридж 100, примерная микросхема 150 памяти, примерный контроллер 306 битовой последовательности, примерный модуль 308 скремблирования битов, примерный интерфейс 310 памяти картриджа, примерный модуль 312 преобразования битовой последовательности, примерный анализатор 314 преобразованной битовой последовательности и/или, в более широком смысле, примерная система 200 аутентификации картриджа, показанная на фиг. 2, могут быть реализованы одной или более аналоговыми или цифровыми схемой(-ами)), логическими схемами, программируемым процессором(-ами), специализированной интегральной микросхемой(-ами) (ASIC), программируемым логическим устройством(-ами) (PLD) и/или программируемой логической интегральной схемой(-ами) (FPLD).

При считывании любого устройства или системы, заявленных в настоящем патенте, чтобы полностью охватить реализацию программного обеспечения и/или встроенного микропрограммного обеспечения, по меньшей мере одно из таких устройств, как примерное устройство 205 формирования изображения, примерный контроллер 220, примерный процессор 225, примерное запоминающее устройство 230 для хранения данных, примерный аутентификатор 240 картриджа, примерное встроенное микропрограммное обеспечение 245 устройства формирования изображения, примерный интерфейс 250 картриджа, примерный картридж 100, примерная микросхема 150 памяти, примерный контроллер 306 битовой последовательности, примерный модуль 308 скремблирования битов, примерный интерфейс 310 памяти картриджа, примерный модуль 312 преобразования битовой последовательности и/или примерный анализатор 314 преобразованной битовой последовательности, таким образом, явно определяются как содержащие физическое считываемое компьютером запоминающее устройство или диск хранения данных, такой как память, цифровой универсальный диск (DVD), компакт-диск (CD), диск Blu-ray и т.д., на которых хранится программное обеспечение и/или встроенные программы. Также, дополнительно, примерная система 200 аутентификации картриджа, показанная на фиг. 2, может содержать один или более элементов, процессов и/или устройств в дополнение или вместо показанных на фиг. 5 и 6, и/или может содержать более одного из любых или всех показанных элементов, процессов и устройств.

Блок-схемы последовательности операций, представляющие примерные

машиночитаемые команды для реализации системы 200 аутентификации картриджа, приведенной на фиг. 2, показаны на фиг. 5 и 6. В этом примере машиночитаемые команды содержат программу, исполняемую процессором, таким как процессор 712, показанный в примерной процессорной платформе 700, обсуждаемой ниже со ссылкой на фиг. 7. Программа может быть введена в программное обеспечение, хранящееся на физическом считываемом компьютером носителе, таком как CD-ROM, дискета, жесткий диск, цифровой универсальный диск (DVD), диск Blu-ray или память, связанная с процессором 712, но вся программа и/или ее части могут альтернативно выполняться устройством, отличным от процессора 712, и/или вводиться во встроенное микропрограммное обеспечение или в назначенное аппаратное обеспечение. Дополнительно, хотя примерная программа описывается со ссылкой на блок-схемы последовательностей выполнения операций, показанные на фиг. 5 и 6, альтернативно может использоваться множество других способов реализации примерной системы 200 аутентификации картриджа. Например, порядок исполнения блоков может быть изменен и/или некоторые из описанных блоков могут быть изменены, удалены или объединены.

Как упомянуто выше, примерные процессы, показанные на фиг. 5 и 6, могут быть реализованы, используя кодированные команды (например, компьютерные и/или машиночитаемые команды), хранящиеся на физическом считываемом компьютером носителе, таком как жесткий диск, флэш-память, постоянное запоминающее устройство (ROM), компакт-диск (CD), цифровой универсальный диск (DVD), кэш, запоминающее устройство с произвольной выборкой (RAM) и/или любое другое запоминающее устройство или диск для хранения данных, на котором в течение любого времени хранится информация (например, в течение расширенных периодов времени, постоянно, в течение кратких моментов, для временного буферирования и/или для кэширования информации). Термин "физический считываемый компьютером носитель для хранения данных", как он используется здесь, явно определяется как содержащий любой тип считываемого компьютером запоминающего устройства и/или диска для хранения данных и исключает распространяющиеся сигналы, а также исключает среду передачи. Здесь термины "физический считываемый компьютером носитель для хранения данных" и "физический машиночитаемый носитель" используются взаимозаменяемо. Дополнительно или альтернативно, примерные процессы, показанные на фиг. 5 и 6, могут быть реализованы, используя кодированные команды (например, считываемые компьютером и/или машиночитаемые команды), хранящиеся на непереносном считываемом компьютером и/или машиночитаемом носителе, таком как жесткий диск, флэш-память, постоянное запоминающее устройство, компакт-диск, цифровой универсальный диск, кэш, запоминающее устройство с произвольной выборкой и/или любое другое запоминающее устройство или диск для хранения данных, где информация хранится в течение любого времени (например, в течение расширенных периодов времени, постоянно, в течение кратких моментов, для временного буферирования и/или для кэширования информации). Термин "постоянный считываемый компьютером носитель", как он используется здесь, явно определяется как содержащий любой тип считываемого компьютером запоминающего устройства и/или диска для хранения данных и исключающий распространяющиеся сигналы и среду передачи. Выражение "по меньшей мере", как оно используется здесь, используется в качестве переходного термина в преамбуле формулы изобретения, оно является открытым на конце таким же образом, как термин "содержащий" является открытым на конце.

На фиг. 5 показана блок-схема последовательности операций, представляющая примерные машиночитаемые команды, которые могут исполняться для реализации

примерной системы аутентификации картриджа, показанной на фиг. 2. Программа, представленная на фиг. 5, начинается с этапа 500, на котором картридж (например, картридж 100) с памятью аутентификации (например, с микросхемой 150 памяти) вставляется в устройство формирования изображения (например, в устройство 205 формирования изображения) (этап 500). В этом примере вставка картриджа запускает интерфейс (например, интерфейс 310 памяти картриджа аутентификатора 240 картриджа) контроллера (например, контроллера 220) устройства формирования изображения, чтобы считать и/или принять битовую последовательность аутентификации памяти аутентификации картриджа (этап 502). В этом примере контроллер устройства формирования изображения определяет скремблирующие биты (например, определяет значения скремблирующих битов) битовой последовательности аутентификации, получая доступ к известным адресным ячейкам битовой последовательности аутентификации (этап 506). В этом примере адресные ячейки скремблирующих битов определяются модулем скремблирующих битов, таким как модуль 308 скремблирующих битов, описанный выше со ссылкой на фиг. 3.

Затем модуль преобразования битовой последовательности (например, модуль преобразования битовой последовательности) аутентификатора картриджа преобразует (например, перестраивает, сдвигает, переставляет и т. д.) битовую последовательность аутентификации, основываясь на скремблирующих битах, на математических операциях со скремблирующими битами и/или на математических операциях между скремблирующими битами и битовой последовательностью аутентификации и/или на любом другом соответствующем преобразовании и/или алгоритме скремблирования (этап 508). В некоторых примерах скремблирующие биты исключаются из этого процесса преобразования. Дополнительно или альтернативно скремблирующие биты определяют или указывают, сколько адресных ячеек для сдвига каждого бита должны перемещаться и/или направление вдоль битовой последовательности, в котором должны перемещаться один или более битов. В некоторых примерах преобразование битовой последовательности аутентификации может происходить посредством многочисленных циклов движения и/или переназначения битов (например, многократно повторяемого рекурсивного процесса). В некоторых примерах, скремблирующие биты, значения скремблирующих битов и/или значения, вытекающие из математических операций со скремблирующими битами, сравниваются с таблицей, чтобы определить алгоритм преобразования, который должен быть применен к битовой последовательности аутентификации. В некоторых примерах, преобразование дополнительно основывается на статических битах битовой последовательности аутентификации.

Преобразованная битовая последовательность аутентификации затем проверяется на правильность, чтобы определить, например, является ли картридж подлинным (этап 510). Как упомянуто выше, эта проверка подлинности может проводиться на преобразованной битовой последовательности, равной ожидаемому значению, контрольным суммам и/или любыми другим соответствующим процессам проверки подлинности. Если картридж определяется как подлинный (этап 512), то использование картриджа с устройством формирования изображения разрешается (этап 514) и процесс завершается (516). Однако, если определяется, что картридж не подлинный (этап 512), процесс завершается (этап 516) до тех пор, пока картридж не будет установлен вновь или пока в устройство формирования изображения не будет вставлен новый картридж.

Хотя пример, показанный на фиг. 5, описывается в отношении проверки подлинности картриджа, примерный процесс и/или части примерного процесса могут также использоваться для шифрования картриджа (например, для записи преобразованной

битовой последовательности аутентификации в память картриджа). Альтернативно, части процесса, показанного на фиг. 5, для других целей могут быть полностью изменены и/или их порядок может быть изменен.

На фиг. 6 представлена другая блок-схема последовательности примерных машиночитаемых команд, которые могут исполняться для реализации примерного картриджа 100 системы 200 аутентификации картриджа, показанной на фиг. 2. В этом примере картридж программируется и/или кодируется битовой последовательностью аутентификации, чтобы не допустить проведение третьими лицами реинжиниринга картриджа и позволить картриджу в дальнейшем проверяться на подлинность устройством формирования изображения. Программа, показанная на фиг. 6, начинается с этапа 600, где картридж (например, картридж 100) подготавливается, например, к программированию, кодированию и/или приему битовой последовательности аутентификации в памяти (например, в микросхеме 150 памяти) (этап 600). В этом примере, определяются скремблирующие биты битовой последовательности аутентификации и/или определяются их значения (этап 602). В частности, адреса скремблирующих битов в показанном примере известны. В некоторых примерах битовая последовательность аутентификации и/или скремблирующие биты определяются и/или обеспечиваются программируемым компьютером и/или устройством.

Затем, в этом примере битовая последовательность аутентификации преобразуется, основываясь на определенных битах скремблирования и/или на определенных значениях скремблирующих битов (этап 604). В некоторых примерах преобразование дополнительно основывается на статических битах битовой последовательности аутентификации. В этом примере статические биты исключаются из процесса преобразования. В некоторых примерах скремблирующие биты находятся в ячейках памяти статических битов. В некоторых примерах скремблирующие биты исключаются из преобразования и используются устройством формирования изображения для проверки подлинности картриджа через другой процесс преобразования (например, дальнейшее преобразование, выполняемое для проверки подлинности картриджа) битовой последовательности аутентификации и/или копии битовой последовательности аутентификации, используемой для проверки подлинности картриджа. Преобразованная битовая последовательность в показанном примере затем записывается (например, кодируется) в память картриджа (этап 606). В частности, программируемое устройство записывает преобразованную битовую последовательность в ROM или EPROM картриджа. После того, как память картриджа запрограммирована, например, посредством программируемого устройства, процесс завершается (этап 608).

На фиг. 7 представлена блок-схема примерной платформы 700 процессора, способной исполнять команды, приведенные на фиг. 5 и 6, чтобы реализовать примерную систему 200 аутентификации картриджа, показанную на фиг. 2. Платформа 700 процессора может быть, например, сервером, персональным компьютером (PC), программатором картриджей, принтером, устройством формирования изображения, мобильным устройством (например, сотовым телефоном, смартфоном, планшетом, таким как iPad™), персональным цифровым помощником (PDA), цифровым видеомагнитофоном интернет-устройства, игровой консолью, персональным видеомагнитофоном, телевизионной приставкой или любым другим типом компьютерного устройства.

Платформа 700 процессора в показанном примере содержит процессор 712. Процессор 712 в показанном примере является аппаратным средством. Например, процессор 712 может быть реализован одной или более интегральными схемами, логическими схемами, микропроцессорами или контроллерами из любого желаемого семейства или от любого

производителя.

Процессор 712 в показанном примере содержит локальную память 713 (например, кэш). Процессор 712 содержит примерный контроллер 220, примерный аутентификатор 240 картриджа, примерный интерфейс 250 картриджа, примерный контроллер 306 битовой последовательности, модуль 308 скремблирующих битов, примерный интерфейс 310 памяти картриджа, примерный модуль 312 преобразования битовой последовательности и примерный анализатор 314 преобразованной битовой последовательности. Процессор 712 в показанном примере осуществляет связь с основной памятью, содержащей энергозависимую память 714 и энергонезависимую память 716, через шину 718. Энергозависимая память 714 может быть реализована синхронной динамической оперативной памятью (SDRAM), динамической оперативной памятью (DRAM), динамической оперативной памятью RAMBUS (RDRAM) и/или любым другим типом устройства оперативной памяти. Энергонезависимая память 716 может быть реализована флэш-памятью и/или любым другим желаемым типом запоминающего устройства. Доступом к основной памяти 714, 716 управляет контроллер памяти.

Платформа 700 процессора в показанном примере также содержит схему 720 интерфейса. Схема 720 интерфейса может быть реализована по любому типу стандарта интерфейса, такому как интерфейс Ethernet, универсальная последовательная шина (USB) и/или экспресс-интерфейс PCI.

В показанном примере одно или более устройств 722 ввода соединяются со схемой 720 интерфейса. Устройство(-а) 722 ввода разрешает(-ют) пользователю вводить данные и команды в процессор 712. Устройство(-а) ввода может быть реализовано, например, аудиодатчиком, микрофоном, камерой (фото- или видео-), клавиатурой, кнопкой, "мышью", сенсорным экраном, сенсорной панелью, шаровым манипулятором, изоэлектрической точкой и/или системой распознавания речи.

В показанном примере одно или более устройств 724 вывода также соединяются со схемой 720 интерфейса. Устройства 724 вывода могут быть реализованы, например, устройствами отображения (например, светодиодом (LED), органическим светодиодом (OLED), жидкокристаллическим дисплеем, электронно-лучевой трубкой (CRT), сенсорным экраном, тактильным устройством вывода, принтером и/или громкоговорителями). Схема 720 интерфейса в показанном примере, таким образом, обычно содержит панель графического драйвера, микросхема графического драйвера или процессор графического драйвера.

Схема 720 интерфейса в показанном примере также содержит устройство связи, такое как передатчик, приемник, приемопередатчик, модем и/или сетевую карту, чтобы облегчить обмен данными с внешними машинами (например, компьютерными устройствами любого вида) через сеть 726 (например, Ethernet-связь, цифровая абонентская линия (DSL), телефонная линия, коаксиальный кабель, сотовая телефонная система и т. д.).

Платформа 700 процессора в показанном примере также содержит одно или более запоминающих устройств большой емкости 728 для хранения программного обеспечения и/или данных. Примерами таких запоминающих устройств 728 большой емкости являются дисководы для дискет, жесткого диска, приводы компакт-диска, приводы дисков Blu-ray, системы RAID и приводы цифровых универсальных дисков (DVD).

Кодированные команды 732, показанные на фиг. 5 и 6, могут храниться в запоминающем устройстве 728 большой емкости, в энергозависимой памяти 714, в энергонезависимой памяти 716 и/или на съемном физическом считываемом компьютером носителе, таком как CD или DVD.

Из вышесказанного должно быть понятно, что раскрытые выше способы, устройства и производственные изделия обеспечивают технологии шифрования для шифрования картриджа и/или для интерпретации памяти аутентификации картриджа, чтобы аутентифицировать картридж при проверке подлинности с помощью устройства формирования изображения. Примеры, раскрытые здесь, могут также уменьшить и/или исключить необходимость передачи и/или обновления ключей шифрования путем определения скремблирующих битов участка памяти аутентификации.

Хотя здесь были раскрыты некоторые примерные способы, устройства и производственные изделия, объем защиты настоящего патента этим не ограничивается. Напротив, этот патент охватывает все способы, устройства и производственные изделия, действительно попадающие в рамки объема защиты формулы изобретения настоящего патента.

(57) Формула изобретения

1. Устройство для аутентификации картриджа с текучей средой, содержащее:

память картриджа с текучей средой, содержащую множество последовательных битов, причем множество последовательных битов включает в себя скремблирующие биты и записывается в память после того, как множество последовательных битов преобразуется рекурсивно, основываясь на скремблирующих битах из множества последовательных битов; и

интерфейс памяти картриджа с текучей средой для разрешения доступа к памяти, чтобы аутентифицировать картридж для текучей среды, посредством верификации множества последовательных битов на основе скремблирующих битов.

2. Устройство по п. 1, в котором множество последовательных битов дополнительно содержит статические биты, которые исключаются из преобразования.

3. Устройство по п. 2, в котором статические биты содержат скремблирующие биты.

4. Устройство по п. 2, в котором множество последовательных битов дополнительно преобразуется, основываясь на статических битах.

5. Устройство по п. 1, в котором память содержит устройство памяти EPROM.

6. Устройство для аутентификации картриджа с текучей средой, содержащее:

структуру данных памяти для памяти картриджа с текучей средой, содержащей множество последовательных битов аутентификации, причем множество последовательных битов аутентификации было преобразовано рекурсивно, основываясь на скремблирующих битах из множества последовательных битов аутентификации, прежде чем множество последовательных битов аутентификации записывается в структуру данных памяти, причем картридж для текучей среды подлежит аутентификации посредством верификации множества последовательных битов аутентификации на основе скремблирующих битов.

7. Устройство по п. 6, в котором множество последовательных битов содержит статические биты, исключенные из преобразования.

8. Устройство по п. 7, в котором статические биты находятся в определенных адресных ячейках памяти.

9. Устройство по п. 7, в котором множество последовательных битов преобразуются, дополнительно основываясь на статических битах.

10. Устройство по п. 6, в котором картридж с текучей средой является неотъемлемой частью сборочного узла схемы печатающей головки картриджа с текучей средой.

11. Устройство по п. 6, в котором память картриджа с текучей средой содержит устройство EPROM.

12. Устройство для аутентификации картриджа с текучей средой, содержащее:

устройство памяти EPROM картриджа с текучей средой, содержащее множество последовательных битов, причем множество последовательных битов включает в себя скремблирующие биты и записывается в устройство памяти EPROM после того, как множество последовательных битов преобразуется рекурсивно, основываясь на скремблирующих битах множества последовательных битов;

электрические контакты картриджа с текучей средой для разрешения доступа к устройству памяти EPROM, чтобы аутентифицировать картридж с текучей средой; и

сборочный узел схемы печатающей головки, электрически соединенной с устройством памяти EPROM и электрическими контактами;

причем картридж для текучей среды подлежит аутентификации посредством верификации множества последовательных битов аутентификации на основе скремблирующих битов.

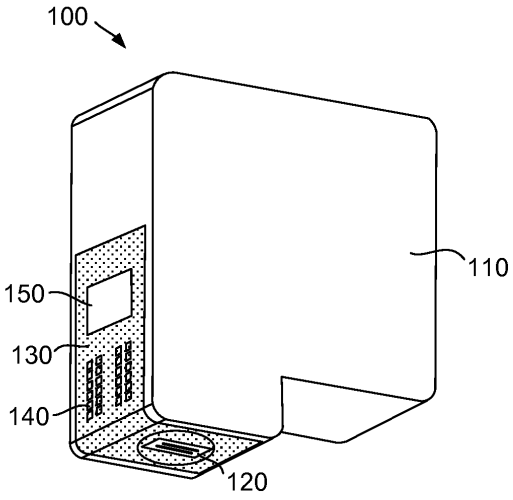
13. Устройство по п. 12, в котором устройство памяти EPROM является неотъемлемой частью сборочного узла схемы печатающей головки.

14. Устройство по п. 12, в котором сборочный узел схемы печатающей головки содержит матрицу печатающей головки.

1

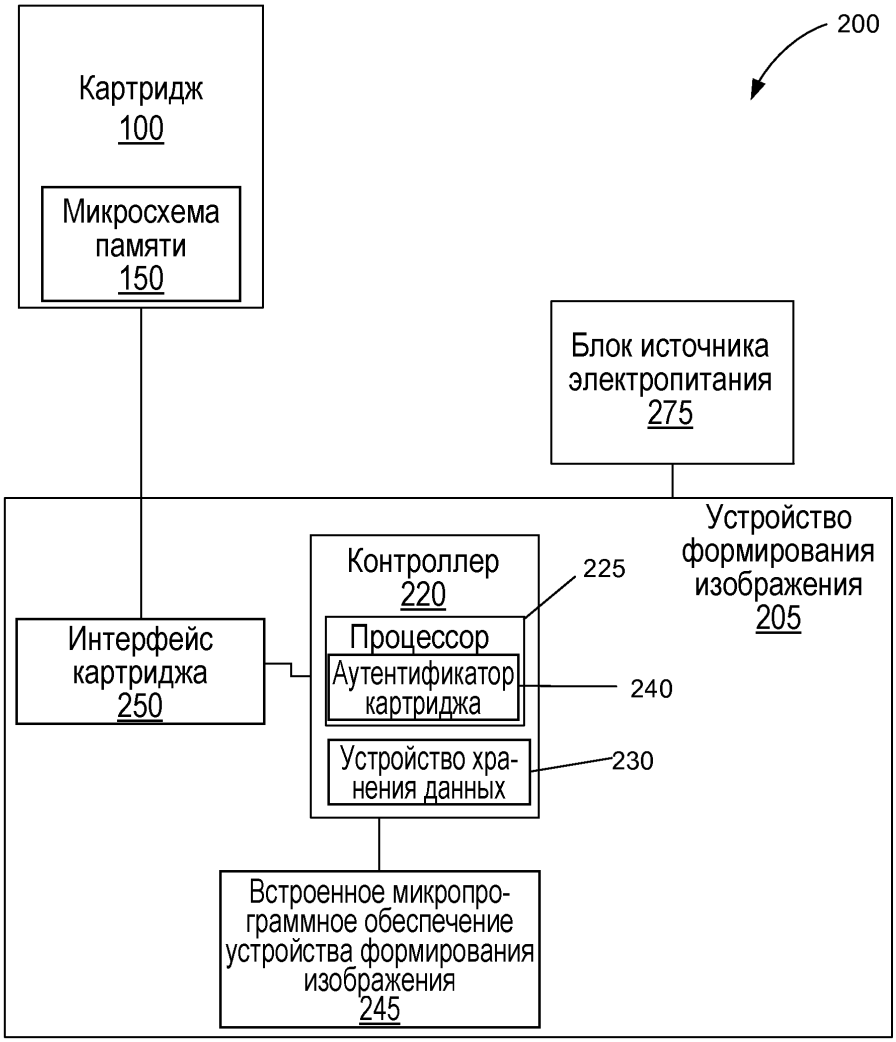
542113

1/7



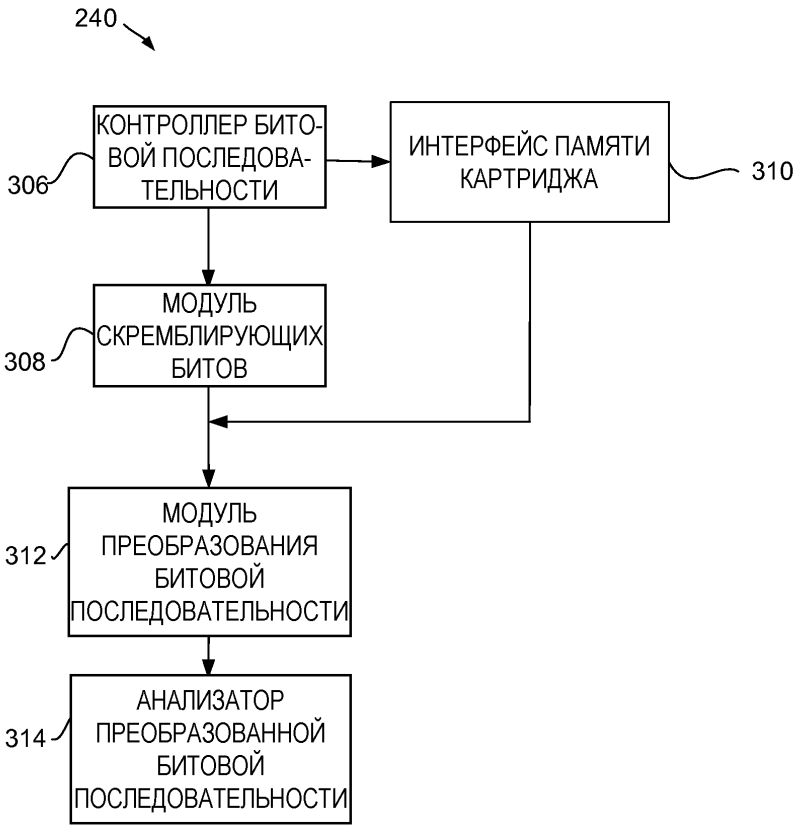
ФИГ. 1

2


200
Картридж
100
Микросхема памяти
150
Блок источника электропитания
275
Устройство формирования изображения
205
Контроллер
220
225
Процессор
Аутентификатор картриджа
240
Интерфейс картриджа
250
Устройство хранения данных
230
Встроенное микропрограммное обеспечение устройства формирования изображения
245

ФИГ. 2

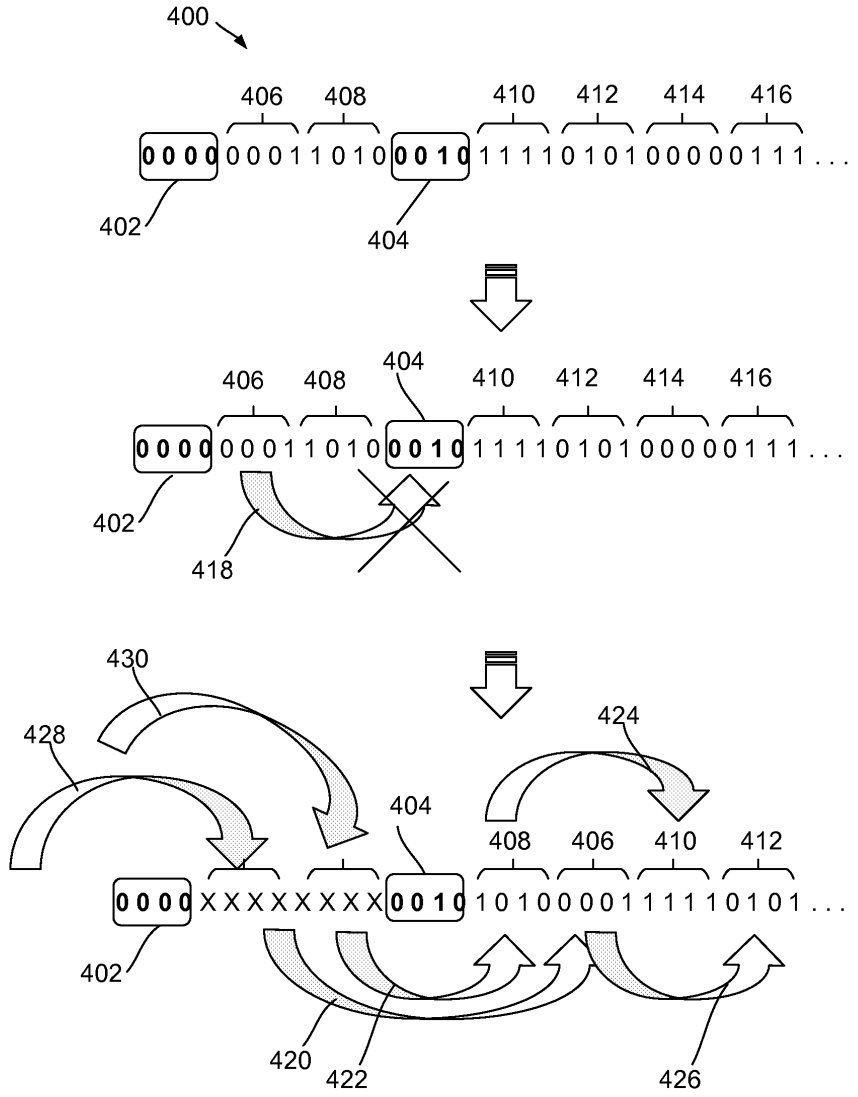
3


240
КОНТРОЛЛЕР БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ
306
ИНТЕРФЕЙС ПАМЯТИ КАРТРИДЖА
310
МОДУЛЬ СКРЕМБЛИРУЮЩИХ БИТОВ
308
МОДУЛЬ ПРЕОБРАЗОВАНИЯ БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ
312
АНАЛИЗАТОР ПРЕОБРАЗОВАННОЙ БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ
314

ФИГ. 3

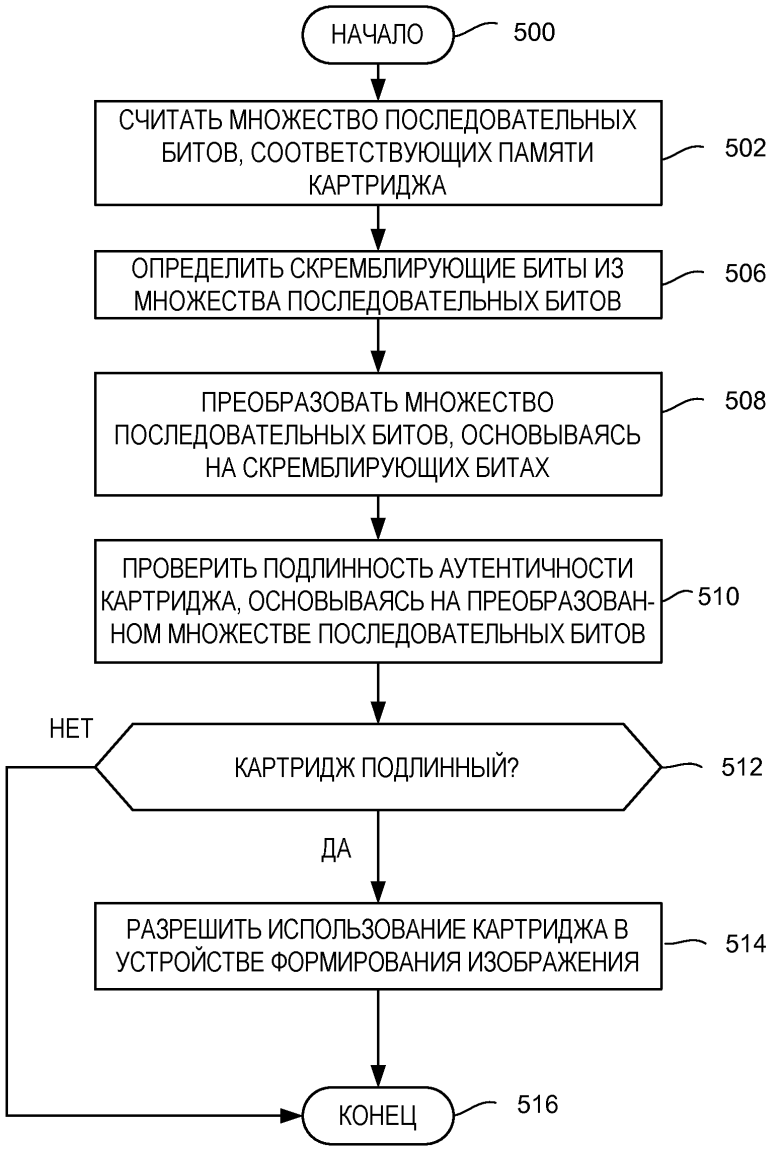
4

4/7


400
406
408
410
412
414
416
0 0 0 0 0 0 0 1 1 0 1 0 0 0 1 0 1 1 1 1 0 1 0 1 0 0 0 0 0 1 1 1 . . .
402
404
406
408
404
410
412
414
416
0 0 0 0 0 0 0 1 1 0 1 0 0 0 1 0 1 1 1 1 0 1 0 1 0 0 0 0 0 1 1 1 . . .
402
418
430
428
424
404
408
406
410
412
0 0 0 0 X X X X X X X X 0 0 1 0 1 0 1 0 0 0 0 1 1 1 1 1 0 1 0 1 . . .
402
420
422
426

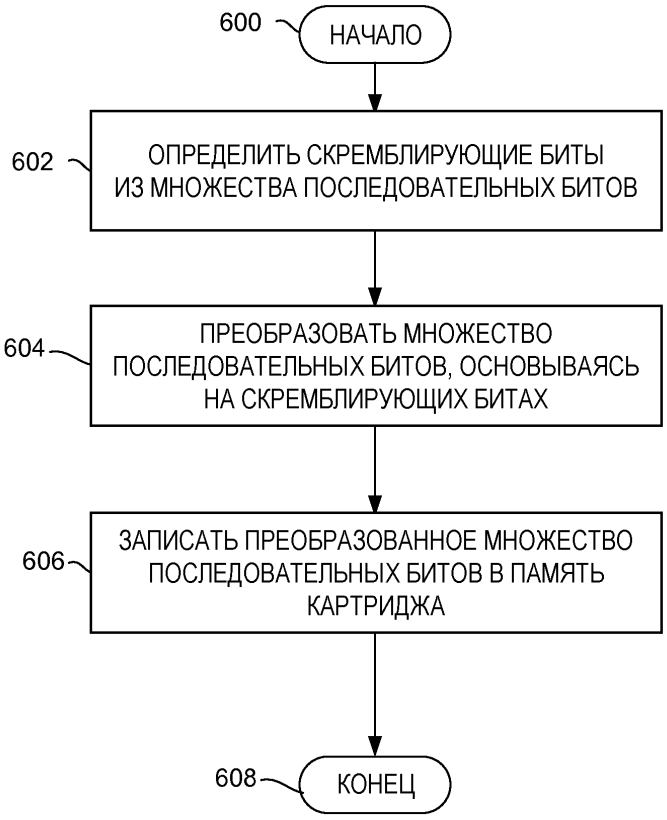
ФИГ. 4

5


НАЧАЛО
500
СЧИТАТЬ МНОЖЕСТВО ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ, СООТВЕТСТВУЮЩИХ ПАМЯТИ КАРТРИДЖА
502
ОПРЕДЕЛИТЬ СКРЕМБЛИРУЮЩИЕ БИТЫ ИЗ МНОЖЕСТВА ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ
506
ПРЕОБРАЗОВАТЬ МНОЖЕСТВО ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ, ОСНОВЫВАЯСЬ НА СКРЕМБЛИРУЮЩИХ БИТАХ
508
ПРОВЕРИТЬ ПОДЛИННОСТЬ АУТЕНТИЧНОСТИ КАРТРИДЖА, ОСНОВЫВАЯСЬ НА ПРЕОБРАЗОВАННОМ МНОЖЕСТВЕ ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ
510
НЕТ
КАРТРИДЖ ПОДЛИННЫЙ?
512
ДА
РАЗРЕШИТЬ ИСПОЛЬЗОВАНИЕ КАРТРИДЖА В УСТРОЙСТВЕ ФОРМИРОВАНИЯ ИЗОБРАЖЕНИЯ
514
КОНЕЦ
516

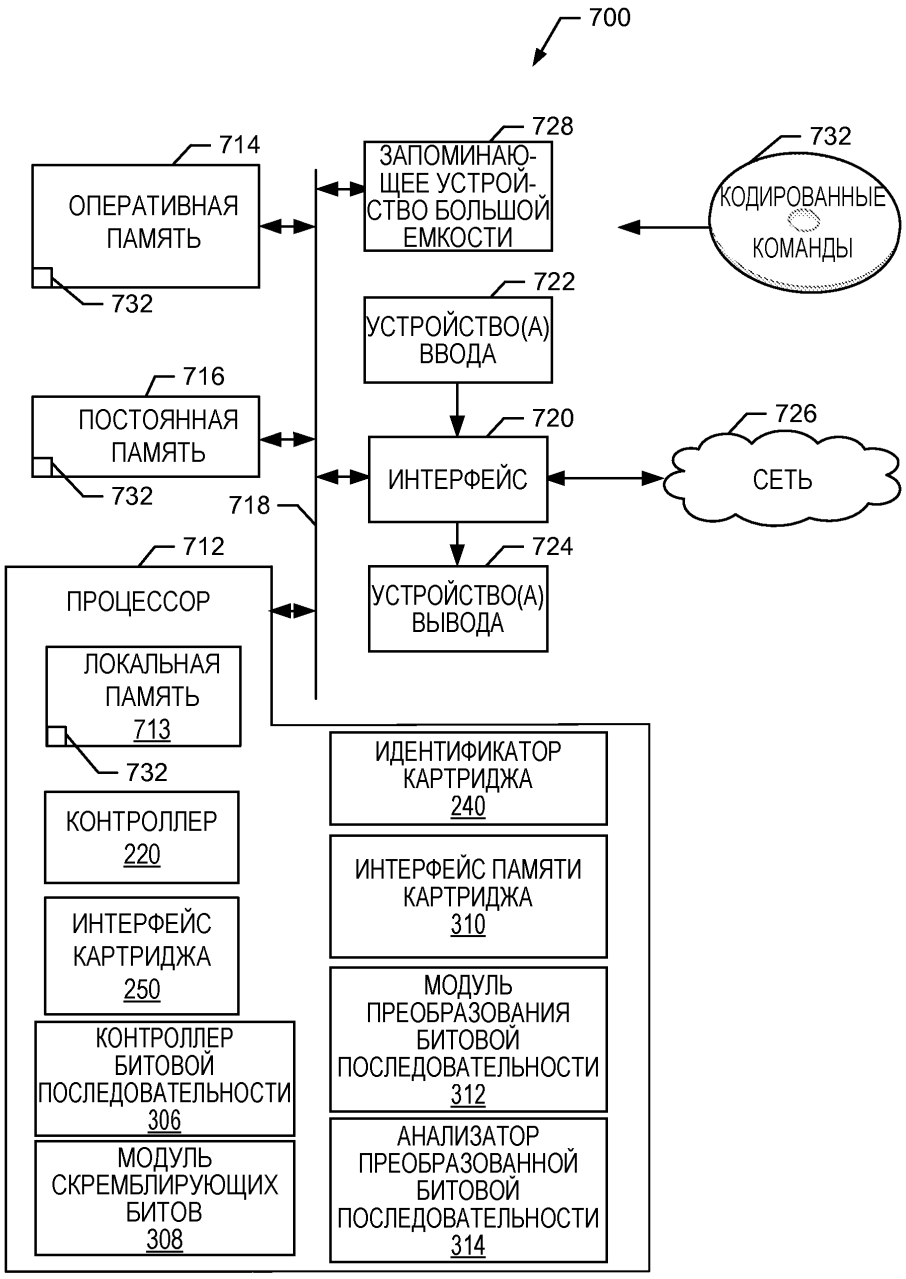
ФИГ. 5

6


600
НАЧАЛО
602
ОПРЕДЕЛИТЬ СКРЕМБЛИРУЮЩИЕ БИТЫ ИЗ МНОЖЕСТВА ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ
604
ПРЕОБРАЗОВАТЬ МНОЖЕСТВО ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ, ОСНОВЫВАЯСЬ НА СКРЕМБЛИРУЮЩИХ БИТАХ
606
ЗАПИСАТЬ ПРЕОБРАЗОВАННОЕ МНОЖЕСТВО ПОСЛЕДОВАТЕЛЬНЫХ БИТОВ В ПАМЯТЬ КАРТРИДЖА
608
КОНЕЦ

ФИГ. 6

7


700
714
ОПЕРАТИВНАЯ ПАМЯТЬ
732
728
ЗАПОМИНАЮЩЕЕ УСТРОЙСТВО БОЛЬШОЙ ЕМКОСТИ
732
КОДИРОВАННЫЕ КОМАНДЫ
722
УСТРОЙСТВО(А) ВВОДА
716
ПОСТОЯННАЯ ПАМЯТЬ
732
720
ИНТЕРФЕЙС
726
СЕТЬ
718
712
ПРОЦЕССОР
724
УСТРОЙСТВО(А) ВЫВОДА
ЛОКАЛЬНАЯ ПАМЯТЬ 713
732
КОНТРОЛЛЕР 220
ИНТЕРФЕЙС КАРТРИДЖА 250
КОНТРОЛЛЕР БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ 306
МОДУЛЬ СКРЕМБЛИРУЮЩИХ БИТОВ 308
ИДЕНТИФИКАТОР КАРТРИДЖА 240
ИНТЕРФЕЙС ПАМЯТИ КАРТРИДЖА 310
МОДУЛЬ ПРЕОБРАЗОВАНИЯ БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ 312
АНАЛИЗАТОР ПРЕОБРАЗОВАННОЙ БИТОВОЙ ПОСЛЕДОВАТЕЛЬНОСТИ 314

ФИГ. 7