(19) Евразийское патентное ведомство

(11) 040711 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.07.20

(21) Номер заявки
202190069

(22) Дата подачи заявки
2019.06.03

(51) Int. Cl. ***G06K 9/00*** (2006.01)
G06F 7/00 (2006.01)

(54) ДВОЙНАЯ МАТЕРИАЛЬНО-ЦИФРОВАЯ ЗАЩИТА ИЗДЕЛИЯ ОТ ПОДДЕЛКИ

(31) **18178639.3**
(32) **2018.06.19**
(33) **EP**
(43) **2021.04.05**
(86) **PCT/EP2019/064366**
(87) **WO 2019/243033 2019.12.26**

(71)(73) Заявитель и патентовладелец:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Деку Эрик, Жилле Филипп, Тевоз Филипп, Уоллес Элизабет (CH)

(74) Представитель:
Рыбина Н.А. (RU)

(56) BENALOH J. ET AL.: "ONE-WAY ACUMULATORS: A DECENTRALIZED ALTERNATIVE TO DIGITAL SIGNATURES (EXTENDED ABSTRACT)", ELECTRONIC PUBLISHING, ARTISTIC IMAGING, AND DIGITAL TYPOGR; [LECTURE NOTES IN COMPUTER SCIENCE, ISSN 0302-9743], SPRINGER VERLAG, DE, vol. 765, 23 May 1993 (1993-05-23), pages 274-285, XP008066935, ISBN: 978-3-540-24128-7 Abstract, sections 1-3 and 5.2

Anonymous: "one way function -Disadvantages of one-way accumulators? -Cryptography Stack Exchange", 12 April 2014 (2014-04-12), XP055528937, Retrieved from the Internet: URL:https://crypto.stackexchange.com/questions/15548/disadvantages-of-one-way-accumulators [retrieved on 2018-11-30] the whole document

KUMAR AMRIT ET AL.: "Performances of cryptographic accumulators", 39TH ANNUAL IEEE CONFERENCE ON LOCAL COMPUTER NETWORKS, IEEE, 8 September 2014 (2014-09-08), pages 366-369, XP032661315, DOI: 10.1109/LCN.2014.6925793 the whole document

DERLER DAVID ET AL.: "Revisiting Cryptographic Accumulators, Additional Properties and Relations to Other Primitives", 11 March 2015 (2015-03-11), INTERNATIONAL CONFERENCE ON SIMULATION, MODELING, AND PROGRAMMING FOR AUTONOMOUS ROBOTS,SIMPAR 2010; [LECTURE NOTES IN COMPUTER SCIENCE; LECT.NOTES COMPUTER], SPRINGER, BERLIN, HEIDELBERG, PAGE(S) 127-144, XP047352728, ISBN: 978-3-642-17318-9 [retrieved on 2015-03-11] the whole document

(57) Изобретение относится к защите изделия от подделки и фальсификации связанных с ним данных и в частности данных, относящихся к его принадлежности к конкретной партии изделий, при этом обеспечивая автономную проверку или проверку в режиме "онлайн" аутентичности защищенного изделия и соответствия связанных с ним данных относительно данных подлинного изделия.

040711 B1

040711 B1

Область техники, к которой относится изобретение

Изобретение относится к области защиты изделий и данных, маркированных на таких изделиях, от подделки или фальсификации, а также соответствия цифровых изображений таких маркированных изделий оригинальным изделиям, и возможности отслеживания изделий.

Уровень техники

Что касается механических деталей, электронных компонентов, фармацевтических продуктов и множества других изделий, то проблемы подделки и фальсификации являются хорошо известными и серьезными, и их количество постоянно растет. Более того, фальсификация данных, связанных с изделием, также является серьезной проблемой. Хорошо известным является пример фальсификации данных, маркированных на оригинальном напечатанном документе, таком как документ, удостоверяющий личность, или диплом (изделие), и дело обстоит еще хуже, если рассматривать цифровую копию или фотокопию оригинального (возможно, подлинного) документа. Простое отслеживание идентификаторов, таких как серийные номера, как правило, является недостаточным решением, поскольку фальсификаторы могут легко скопировать такие номера.

Существует множество других схем защиты для производственных изделий, но они, как правило, не обеспечивают достаточного уровня защиты, у них слишком высокие административные накладные расходы с точки зрения информации, которую необходимо хранить и к которой необходимо получать доступ, они часто непрактичны для использования, кроме как в хорошо контролируемых средах, или они просто не могут быть реализованы физически. Например, многие схемы цифровой защиты документов поддающимся верификации способом не подходят для использования в контекстах, в которых задействовано множество физических товаров, которые нецелесообразно или иным образом нежелательно маркировать соответствующими подписями.

Другим недостатком большинства традиционных методов обеспечения аутентичности изделий или защиты связанных с ними данных является то, что они склонны просматривать изделия изолированно, даже если они являются членами четко определенной группы, например, производственной партии. Это игнорирует ценную аутентификационную информацию.

Обычным способом защиты изделия является нанесение на него защитной маркировки на основе материала (возможно, защищенной от несанкционированного доступа), то есть маркировки, обладающей обнаруживаемым внутренним физическим или химическим свойством, которое очень трудно (если не невозможно) воспроизвести. Если пригодный датчик обнаруживает это внутреннее свойство маркировки, данная маркировка считается подлинной с высокой степенью достоверности, а следовательно, и соответствующее маркированное изделие. Существует множество примеров таких известных аутентифицирующих внутренних свойств: маркировка может включать некоторые частицы, возможно, распределенные случайным образом, или имеет определенную слоистую структуру, имеющую внутренние свойства оптического отражения, или пропускания, или поглощения, или даже испускания (например, люминесценцию, или поляризацию, или дифракцию, или препятствие и т.д.), возможно обнаруживаемые при определенных условиях освещения "светом" определенного спектрального состава. Это внутреннее свойство может быть результатом особого химического состава материала маркировки: например, люминесцентные пигменты (возможно, не коммерчески доступные) могут быть диспергированы в краске, используемой для печати некоторого рисунка на изделии, и используются для испускания определенного света (например, в спектральном окне в пределах инфракрасного диапазона) при освещении определенным светом (например, светом в УФ спектральном диапазоне). Это используется, например, для защиты банкнот. Можно использовать и другие внутренние свойства: например, люминесцентные частицы в маркировке могут иметь определенное время затухания люминесцентного испускания после освещения пригодным возбуждающим световым импульсом. Другими типами внутренних свойств являются магнитное свойство включенных частиц или даже свойство "отпечатка пальца" самого изделия, такое как, например, относительное расположение изначально распределенных случайным образом волокон бумажной подложки документа в заданной зоне на документе, который при просмотре с достаточным разрешением может служить для извлечения уникальной характеристической подписи или некоторых случайных печатных артефактов данных, напечатанных на изделии, которые при просмотре с достаточным увеличением также могут привести к уникальной подписи и т. д. Основная проблема, связанная с внутренним свойством отпечатка пальца изделия, это его устойчивость к старению или износу. Однако, защитная маркировка на основе материала не всегда позволяет также защитить данные, связанные с маркированным изделием: например, даже если документ маркирован защитной маркировкой на основе материала, такой как логотип, напечатанный защитной краской в некоторой зоне документа, данные, напечатанные на оставшейся части документа, могут быть сфальсифицированы. Более того, слишком сложные аутентифицирующие подписи часто требуют значительных хранилищ с участием внешних баз данных и каналов связи для запросов к таким базам данных, так что автономная аутентификация изделия невозможна.

Таким образом, целью настоящего изобретения является защита изделия от подделки и фальсификации связанных с ним данных и, в частности, данных, относящихся к его принадлежности к определенной партии изделий. Также целью настоящего изобретения является обеспечение возможности автоном-

ной проверки аутентичности объекта, защищенного согласно настоящему изобретению, и соответствия связанных с ним данных данным подлинного объекта.

Краткое описание изобретения

Один из аспектов настоящего изобретения относится к способу защиты заданного оригинального изделия из партии множества оригинальных изделий от подделки или фальсификации, при этом каждое оригинальное изделие партии имеет собственные связанные с ним данные изделия и соответствующие цифровые данные изделия, при этом способ включает этапы: для каждого оригинального изделия партии, вычисления посредством односторонней функции связанной с изделием цифровой подписи его соответствующих цифровых данных изделия; вычисления контрольной агрегированной цифровой подписи, соответствующей партии оригинальных изделий, из всех цифровых подписей оригинальных изделий партии посредством одностороннего сумматора указанных цифровых подписей изделий, и предоставления в распоряжение пользователя контрольной агрегированной цифровой подписи; определения ключа верификации изделия, соответствующего цифровой подписи указанного заданного оригинального изделия, посредством частичного одностороннего сумматора других цифровых подписей изделий, используемых для вычисления контрольной агрегированной цифровой подписи, в результате чего потенциальная цифровая подпись изделия соответствует подписи оригинального изделия партии, в случае извлечения контрольной агрегированной цифровой подписи из односторонней функции указанной потенциальной цифровой подписи изделия и соответствующего ключа верификации изделия; и нанесения на заданное оригинальное изделие соответствующей машиночитаемой защитной маркировки изделия, включающей представление связанных с изделием цифровых данных и его соответствующего ключа верификации изделия, тем самым получая маркированное оригинальное изделие, данные изделия которого защищены от подделки или фальсификации.

Контрольная агрегированная цифровая подпись, связанная с партией оригинальных изделий, может быть либо опубликована в среде, открытой для пользователя, либо сохранена в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, либо сохранена в блокчейне, либо сохранена в базе данных, защищенной блокчейном, открытой для пользователя. Более того, маркированное оригинальное изделие может дополнительно содержать данные по доступу к агрегированным подписям, маркированные на нем и содержащие информацию, достаточную для получения доступа к контрольной агрегированной цифровой подписи, соответствующей партии оригинальных изделий, при этом указанная информация представляет собой ссылку в интерфейс сбора агрегированных подписей, соответственно, одного из следующего: среда, в которой опубликована контрольная агрегированная цифровая подпись, при этом среда является открытой для пользователя посредством указанного интерфейса сбора агрегированных подписей, выполненного с возможностью приема от пользователя запроса на агрегированную подпись, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной агрегированной цифровой подписи связанной партии; доступная для поиска база данных агрегированных подписей, в которой сохранена контрольная агрегированная цифровая подпись, при этом база данных агрегированных подписей является открытой для пользователя посредством указанного интерфейса сбора агрегированных подписей, выполненного с возможностью приема от пользователя запроса на агрегированную подпись, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной агрегированной цифровой подписи связанной партии; блокчейн, соответственно, база данных, защищенная блокчейном, в котором сохранена агрегированная цифровая подпись с временной меткой, при этом блокчейн, соответственно, база данных, защищенная блокчейном, является открытым для пользователя посредством указанного интерфейса сбора агрегированных подписей, выполненного с возможностью приема от пользователя запроса на агрегированную подпись, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной агрегированной цифровой подписи связанной партии.

Согласно настоящему изобретению виртуальное изделие может быть включено в партию оригинальных изделий, при этом указанное виртуальное изделие имеет связанные с виртуальным изделием данные и его соответствующие цифровые данные виртуального изделия, а также связанную с виртуальным изделием цифровую подпись, получаемую посредством односторонней функции, при этом указанное виртуальное изделие не создается, а только используется для генерирования связанной с виртуальным изделием цифровой подписи из соответствующих цифровых данных виртуального изделия; контрольная агрегированная цифровая подпись, связанная с указанной партией оригинальных изделий, вычислена из всех цифровых подписей оригинальных изделий партии, включающих цифровую подпись виртуального изделия, посредством одностороннего сумматора.

Односторонняя функция может представлять собой хеш-функцию, а цифровая подпись оригинального изделия может представлять собой последовательность заданного множества битов с меньшими значениями разряда, выбранных из битов хеш-значения соответствующих цифровых данных изделия.

В вышеуказанном способе дополнительные цифровые данные изделия, соответствующие данным

изделия, связанным с маркированным оригинальным изделием, могут быть сохранены в доступной для поиска информационной базе данных, открытой для пользователя, посредством интерфейса информационной базы данных, выполненного с возможностью приема от пользователя запроса на информацию, содержащего данные изделия или соответствующие данные цифровой подписи, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно соответствующих дополнительных цифровых данных изделия.

Маркированное оригинальное изделие может дополнительно содержать соответствующую маркировку данных изделия, нанесенную на него, при этом указанная маркировка данных изделия включает соответствующие данные изделия, связанные с указанным маркированным оригинальным изделием.

Цифровые данные маркированного оригинального изделия могут включать контрольные физические характеристические цифровые данные UPC соответствующей уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека. Более того, уникальная физическая характеристика маркированного оригинального изделия может представлять собой характеристику защитной маркировки на основе материала, нанесенной на оригинальное изделие.

Другой аспект настоящего изобретения относится к способу верификации аутентичности изделия, защищенного согласно вышеупомянутому способу защиты оригинального изделия, или соответствия копии такого защищенного изделия относительно оригинального изделия, при этом способ включает этапы, при рассматривании тестового объекта, представляющего собой указанное изделие или указанную копию изделия: получения цифрового изображения защитной маркировки на тестовом объекте посредством устройства для формирования изображения, имеющего блок формирования изображения, ЦП с памятью и блок обработки изображения; считывания представления цифровых данных изделия и связанного с изделием ключа верификации на полученном цифровом изображении защитной маркировки на тестовом объекте и извлечения, соответственно, соответствующих цифровых данных изделия и ключа верификации изделия из указанного считанного представления; сохранения в памяти контрольной агрегированной цифровой подписи соответствующей партии изделий и программирования в ЦП односторонней функции и одностороннего сумматора; верификации действительного соответствия извлеченных цифровых данных изделия и связанного с изделием ключа верификации сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов: вычисления цифровой подписи извлеченных цифровых данных изделия с помощью односторонней функции; вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных изделия и извлеченного ключа верификации изделия с помощью одностороннего сумматора; и проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего, в случае совпадения указанных агрегированных цифровых подписей, данные изделия на тестовом объекте являются данными подлинного оригинального изделия.

Способ верификации, в котором изделие защищено путем сохранения контрольной агрегированной цифровой подписи, связанной с партией оригинальных изделий, в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, и в котором устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, может включать предварительные этапы: отправки блоком связи посредством канала связи запроса в указанную базу данных агрегированных подписей и приема обратно контрольной агрегированной цифровой подписи, связанной с партией оригинальных изделий; и сохранения принятой агрегированной цифровой подписи в памяти устройства для формирования изображения.

В способе верификации изделие может быть защищено путем включения данных по доступу к агрегированным подписям, как упомянуто выше, и устройство для формирования изображения может быть дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, при этом способ верификации включает предварительные этапы: считывания данных по доступу к агрегированным подписям, маркированных на тестовом объекте, с помощью устройства для формирования изображения; отправки блоком связи посредством канала связи запроса на агрегированную подпись в указанный интерфейс сбора агрегированных подписей, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующей контрольной агрегированной цифровой подписи связанной партии; и сохранения принятой агрегированной цифровой подписи в памяти устройства для формирования изображения.

Изделие может быть защищено дополнительными данными изделия, как упомянуто выше, и устройство для формирования изображения может дополнительно быть оснащено средствами связи, выполненными с возможностью отправки в интерфейс информационной базы данных запроса на информацию, содержащего данные изделия или соответствующие данные цифровой подписи, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующих дополнительных цифровых данных изделия.

Изделие может быть защищено маркировкой данных изделия, как упомянуто выше, при этом спо-

соб верификации включает дополнительные этапы: считывания данных изделия, маркированных на маркировке данных изделия на тестовом объекте, с помощью устройства для формирования изображения; и проверки соответствия данных изделия, считанных из маркировки данных изделия, цифровым данным изделия, извлеченным из защитной маркировки на тестовом объекте.

Изделие может быть защищено маркировкой данных изделия и может дополнительно иметь защитную маркировку на основе материала, как упомянуто выше, и устройство для формирования изображения может дополнительно быть оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека, и ЦП запрограммирован для извлечения соответствующих цифровых данных уникальной физической характеристики из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные физические характеристические цифровые данные UPC, соответствующие указанной уникальной физической характеристике маркированного оригинального изделия или связанного объекта или человека, при этом способ включает дополнительные этапы, при рассматривании субъекта, представляющего собой указанное изделие или указанный связанный объект или человека: обнаружения с помощью датчика уникальной физической характеристики субъекта и извлечения соответствующих потенциальных цифровых данных уникальной физической характеристики UPC^c; сравнения полученных потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC; и в случае схожести потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC, при условии заданного критерия допустимого отклонения, субъект считается подлинным.

Другой аспект настоящего изобретения относится к способу верификации соответствия цифрового изображения оригинального изделия, защищенного согласно вышеупомянутому способу, относительно маркированного оригинального изделия, при этом способ включает этапы: приема цифрового изображения изделия, демонстрирующего защитную маркировку на оригинальном изделии, посредством устройства для формирования изображения, имеющего блок формирования изображения, ЦП с памятью и блок обработки изображения; считывания представления цифровых данных изделия и связанного с изделием ключа верификации на полученном цифровом изображении защитной маркировки и извлечения, соответственно, соответствующих цифровых данных изделия и ключа верификации изделия из указанного считанного представления; сохранения в памяти контрольной агрегированной цифровой подписи соответствующей партии изделий и программирования в ЦП односторонней функции и одностороннего сумматора; верификации действительного соответствия извлеченных цифровых данных изделия и связанного ключа верификации сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов: вычисления цифровой подписи извлеченных цифровых данных изделия с помощью односторонней функции; вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных изделия и извлеченного ключа верификации с помощью одностороннего сумматора; и проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего, в случае совпадения указанных агрегированных цифровых подписей, данные изделия на цифровом изображении изделия являются данными подлинного оригинального изделия.

Изделие может быть защищено путем сохранения контрольной агрегированной цифровой подписи, связанной с партией оригинальных изделий, в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, как раскрыто выше, и устройство для формирования изображения может дополнительно быть оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, при этом способ верификации соответствия включает предварительные этапы: отправки блоком связи посредством канала связи запроса в указанную базу данных агрегированных подписей и приема обратно контрольной агрегированной цифровой подписи, связанной с партией оригинальных изделий; и сохранения принятой агрегированной цифровой подписи в памяти устройства для формирования изображения.

В варианте изделие может быть защищено данными по доступу к агрегированным подписям, как упомянуто выше, и устройство для формирования изображения может дополнительно быть оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, при этом способ верификации соответствия включает предварительные этапы: считывания данных по доступу к агрегированным подписям с помощью устройства для формирования изображения на принятом цифровом изображении изделия, демонстрирующем данные по доступу, маркированные на изделии; отправки блоком связи посредством канала связи запроса на агрегированную подпись в указанный интерфейс сбора агрегированных подписей, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из изображения защитной маркировки на изделии, и приема обратно соответствующей контрольной агрегированной цифровой подписи связанной партии; и сохранения принятой агрегированной цифровой подписи в памяти устройства для формирования изображения.

Изделие может быть защищено маркировкой данных изделия, как раскрыто выше, и способ верификации соответствия цифрового изображения изделия может включать дополнительные этапы: считы-

вания данных изделия, маркированных на маркировке данных изделия, на принятом цифровом изображении изделия с помощью устройства для формирования изображения; и проверки соответствия данных изделия, считанных из цифрового изображения маркировки данных изделия, цифровым данным изделия, извлеченным из защитной маркировки на принятом цифровом изображении изделия.

Согласно еще одному аспекту настоящее изобретение относится к маркированному изделию, принадлежащему к партии множества оригинальных изделий и защищенному от подделки или фальсификации согласно вышеупомянутому способу, при этом каждое оригинальное изделие партии имеет собственные связанные с ним данные изделия и соответствующие цифровые данные изделия, указанная партия имеет соответствующую контрольную агрегированную цифровую подпись, при этом изделие содержит: машиночитаемую защитную маркировку, нанесенную на него и включающую представление связанных с изделием цифровых данных и соответствующего ключа верификации изделия.

Цифровые данные маркированного изделия могут включать контрольные физические характеристические цифровые данные UPC соответствующей уникальной физической характеристики маркированного изделия или связанного объекта или человека.

Уникальная физическая характеристика маркированного изделия может представлять собой характеристику защитной маркировки на основе материала, нанесенной на маркированное изделие.

Настоящее изобретение дополнительно относится к системе верификации аутентичности маркированного оригинального изделия, защищенного согласно вышеупомянутому способу защиты, или соответствия копии такого изделия относительно оригинального изделия, при этом система содержит устройство для формирования изображения, имеющее блок формирования изображения, ЦП с памятью и блок обработки изображения, при этом память сохраняет контрольную агрегированную цифровую подпись соответствующей партии изделий и одностороннюю функцию и односторонний сумматор, запрограммированные в ЦП, при этом система выполнена с возможностью: получения цифрового изображения защитной маркировки на тестовом объекте, представляющем собой указанное изделие или указанную копию изделия; считывания представления цифровых данных изделия и связанного с изделием ключа верификации на полученном цифровом изображении защитной маркировки на тестовом объекте и извлечения, соответственно, соответствующих цифровых данных изделия и ключа верификации изделия из указанного считанного представления; верификации действительного соответствия извлеченных цифровых данных изделия и связанного ключа верификации сохраненной контрольной агрегированной цифровой подписи путем осуществления на ЦП дополнительных запрограммированных этапов: вычисления цифровой подписи извлеченных цифровых данных изделия с помощью односторонней функции; вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных изделия и извлеченного ключа верификации с помощью одностороннего сумматора; и проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего, в случае совпадения указанных агрегированных цифровых подписей, система выполнена с возможностью доставки указания того, что данные изделия на тестовом объекте являются данными подлинного оригинального изделия.

В вышеупомянутой системе для верификации изделия, защищенного контрольными физическими характеристическими цифровыми данными UPC, которые могут относиться к защитной маркировке на основе материала, как раскрыто выше, устройство для формирования изображения может дополнительно быть оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека, и ЦП запрограммирован для извлечения соответствующих цифровых данных уникальной физической характеристики из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные физические характеристические цифровые данные UPC, соответствующие указанной уникальной физической характеристике маркированного оригинального изделия или связанного объекта или человека, при этом система дополнительно выполнена с возможностью: обнаружения с помощью датчика уникальной физической характеристики субъекта, представляющего собой указанное изделие или указанный связанный объект или человека, и извлечения соответствующих потенциальных цифровых данных уникальной физической характеристики UPC^c; сравнения полученных потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC; и в случае схожести потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC, при условии заданного критерия допустимого отклонения, доставки указания того, что субъект считается подлинным.

Настоящее изобретение также относится к системе верификации соответствия цифрового изображения оригинального изделия, защищенного согласно вышеупомянутому способу защиты, относительно маркированного оригинального изделия, при этом система содержит устройство для формирования изображения, имеющее блок формирования изображения, ЦП с памятью и блок обработки изображения, при этом память сохраняет контрольную агрегированную цифровую подпись соответствующей партии изделий и одностороннюю функцию и односторонний сумматор, запрограммированные в ЦП, при этом система выполнена с возможностью: приема цифрового изображения изделия, демонстрирующего за-

щитную маркировку на оригинальном изделии; считывания представления цифровых данных изделия и связанного с изделием ключа верификации на полученном цифровом изображении защитной маркировки и извлечения, соответственно, соответствующих цифровых данных изделия и ключа верификации изделия из указанного считанного представления; верификации действительного соответствия извлеченных цифровых данных изделия и связанного ключа верификации сохраненной контрольной агрегированной цифровой подписи путем осуществления на ЦП дополнительных запрограммированных этапов: вычисления цифровой подписи извлеченных цифровых данных изделия с помощью односторонней функции; вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных изделия и извлеченного ключа верификации с помощью одностороннего сумматора; и проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего, в случае совпадения указанных агрегированных цифровых подписей, система выполнена с возможностью доставки указания того, что данные изделия на цифровом изображении изделия являются данными подлинного оригинального изделия.

Далее настоящее изобретение будет описано более полно со ссылкой на прилагаемые чертежи, на которых проиллюстрированы основные аспекты и признаки настоящего изобретения.

Краткое описание чертежей

На фиг. 1 представлен схематический вид общего способа защиты партии изделий согласно настоящему изобретению.

На фиг. 2A проиллюстрирован защищенный биометрический паспорт в качестве примера биометрического документа, удостоверяющего личность, защищенного согласно настоящему изобретению.

На фиг. 2B проиллюстрирован контроль человека, имеющего защищенный биометрический паспорт согласно фиг. 2A, уполномоченным сотрудником.

На фиг. 3 проиллюстрирована партия компонентов самолета, защищенных согласно настоящему изобретению.

На фиг. 4 проиллюстрирована партия фармацевтических продуктов, защищенных согласно настоящему изобретению.

Подробное описание

Настоящее изобретение в данном случае подробно описано со ссылкой на неограничивающие варианты осуществления, проиллюстрированные на чертежах.

На фиг. 1 проиллюстрирован общий способ согласно настоящему изобретению, относящийся к защите партии изделий, и к способу вычисления кодирования верифицированной информации, которая может быть связана с каждым изделием. На фиг. 1 проиллюстрирована группа или "партия" изделий A_1, A_2 A_3, ..., которые могут представлять собой что угодно, способное нести или содержать физическую машиночитаемую защитную маркировку 110 (в данном случае проиллюстрированную двухмерным штрих-кодом) или нести нечто, что, в свою очередь, несет или содержит физическую защитную маркировку. Изделие может представлять собой промышленный товар или его упаковку, физический документ или изображение, упаковку, содержащую несколько товаров (например, блистерную упаковку с лекарством), или контейнер, содержащий поддоны с картонными коробками с товарами и т.д. Даже человек или животное могут быть "изделием" в контексте вариантов осуществления настоящего изобретения; например, авторизованные участники мероприятия или члены группы, или члены стада или стаи могут иметь при себе какой-либо идентификационный значок или (особенно в случае животных) иметь физическую маркировку.

Партия может, например, относиться к обычному производственному циклу, товарам, доставленным конкретным поставщиком, товарам, изготовленным или отправленным в течение определенного периода времени, набору связанных изображений, группе людей, стаду или стае или любой другой определяемой пользователем группировке любых объектов, для которых могут быть определены данные A_i. На фиг. 1 также показано "виртуальное изделие" A_v, которое является необязательным средством программного обеспечения, которое может быть включено для обеспечения кодирования выбранных данных. Это объясняется далее. Исключительно для примера предполагается, что виртуальное изделие A_v включено и будет рассматриваться ниже как другие изделия A_1, A_2, A_3, ..., поскольку оно может обрабатываться практически таким же образом (хотя оно не соответствует реальному объекту). Конечно, множество виртуальных изделий A_{v1}, A_{v2}, ...,A_{vk} можно использовать для кодирования цифровых данных и создания более надежных цифровых подписей изделия (см. ниже).

Для каждого изделия A_1, A_2, A_3, ... A_v соответствующие цифровые данные изделия D_1, D_2, D_3, ... , D_v связаны или извлечены (или, в случае виртуального изделия A_v, созданы) с помощью любого пригодного способа. Эти данные могут представлять собой некоторую меру физических характеристик, текстовые данные, такие как заполненная форма или информация о продукте, серийный номер или другой идентификатор, указания содержимого, цифровое представление изображения или любая другая информация, которую разработчик системы решает связать с изделием. Цифровые данные изделия D_i могут быть извлечены из читаемых человеком данных (например, буквенно-цифровых данных), маркированных на изделии (например, напечатанных на изделии или на этикетке, прикрепленной к изделию) посредством

считывателя, выполненного с возможностью создания соответствующего файла цифровых данных. Дополнительные цифровые данные (например, команда для использования изделия или команды безопасности и т.д.) могут быть связаны с извлеченными данными для создания цифровых данных изделия D_i.

Для виртуального изделия A_v связанные цифровые данные могут включать, например, идентификационный номер партии, количество изделий в партии, (псевдо-) рандомный номер с целью увеличения защиты путем увеличения энтропии данных, информации о дате и/или времени, и т.д. Еще одной формой связанных данных могут быть указания допустимых или недопустимых правил операций, дат истечения срока действия и т. д. Короче говоря, цифровые данные D_v могут быть чем угодно, что может быть представлено в цифровой форме.

Для каждого изделия его соответствующие цифровые данные изделия D_1, D_2, D_3, ..., D_v предпочтительно преобразовываются математическим путем, так что они по существу скрыты, хотя это не является абсолютным требованием для любого варианта осуществления. Это преобразование, применяемое к цифровым данным D_i изделия A_i, служит для создания соответствующей цифровой подписи x_i. Эту цифровую подпись получают посредством односторонней функции (то есть функции, которую легко вычислить, но трудно инвертировать, см. S. Goldwasser and M. Bellare "Lecture Notes on Cryptography", MIT, июль 2008 г, http://www-cse.ucsd.edu/users/mihir).

Одним из таких выгодных преобразований является, например, применение хеш-функции H( ) = hash( ) к цифровым данным изделия, которая обычно имеет свойство возвращать выходные данные известной длины в битах независимо от размера входных данных: этот технический эффект особенно полезен для создания цифровой подписи цифровых данных, связанных с изделием, независимо от размера связанных цифровых данных изделия и размера партии. Хеш-функция - это хорошо известный пример односторонней функции. Если используется криптографическая хеш-функция, такая как класс функций SHA (Secure Hash Algorithm), например SHA-256, то существуют дополнительные преимущества, заключающиеся в том, что функция практически необратима и устойчива к коллизиям, то есть вероятность того, что две разные группы входных данных приведут к одним и тем же выходным данным, ничтожна. Как будет понятно из приведенного ниже описания, это также не является требованием настоящего изобретения, хотя оно выгодно по тем же причинам, что и в других приложениях. Как показано на фиг. 1, значения x_1, x_2, x_3,..., x_v представляют собой хеш-значения, то есть связанные с изделиями цифровые подписи соответственных наборов данных изделия, то есть $x_j = H(D_j)$, для j=1, ..., v. Для краткости X (заглавная буква) используется в данном случае и на фиг. 1 для обозначения набора хешированных значений данных; таким образом, $X = (x_1, x_2, ..., x_v)$ (если включено виртуальное изделие A_v; в противном случае, элемент x_v можно опустить).

Чтобы сократить подпись, цифровая подпись x_j изделия A_j может даже быть просто последовательностью заданного множества битов с меньшими значениями разряда, выбранных из битов хеш-значения $H(D_j)$: например, с помощью хеш-функции SHA-256 семейства SHA-2, достаточно сохранить только 128 битов с меньшими значениями разряда из 256 бит подписи, чтобы по-прежнему иметь надежную подпись в отношении криптоаналитической атаки.

Агрегированную цифровую подпись или значение партии B затем вычисляют по X посредством (квази-коммутативного) одностороннего сумматора (см. статью Josh Benaloh and Michael de Mare "One-Way Accumulators: A Decentralized Alternative to Digital Signatures", Advances in Cryptology - Eurocrypt' 93, LNCS, выпуск 765, страницы 274-285, Springer-Verlag, 1993 г. и статью "one way function - Disadvantages of one-way accumulators? - Cryptography Stack Exchange" неизвестного автора, от 12 апреля 2014 г.). В общем, для набора μ подписей x_1,x_2, ...x_μ (возможно в том числе цифровых подписей одного или более виртуальных изделий), соответствующее суммарное значение $f(x_1, x_2, ... x_\mu)$, сокращено как f(X) с $X = (x_1, x_2, ... x_\mu)$, заданное односторонним сумматором f, представляет собой:

$$f(x_1, x_2, \ldots . x_\mu) = f(f(f(\ldots f(f(f(x_1), x_2) \ldots x_3), \ldots, x_{\mu-2}), x_{\mu-1}), x_\mu).$$

В общем, можно написать $f(x_1, x_2) = x_1 \otimes x_2$, где ⊗ является связанным оператором, предпочтительно выбранным таким образом, чтобы f(X) было достаточно трудно инвертировать, чтобы вычислительная нагрузка была слишком высокой при практической реализации. Эта концепция вычислительной непрактичности, используемая в вариантах осуществления, дополнительно раскрыта ниже. Согласно настоящему изобретению односторонний сумматор выбран для вычисления агрегированных подписей ввиду условия ограничения размера B. Фактически, такой сумматор создает цифровое значение, размер которого (то есть количество битов) не зависит от размера его аргументов.

В качестве элементарного примера значение партии может быть функцией f(X), такой как коммутативное сложение по модулю заданного модуля m, то есть $f(x) = x \bmod m$ и $f(x, y) = x \otimes y$, со связанным коммутирующим оператором ⊗, определенным $x \otimes y = (x + y) \bmod m$. Таким образом, в данном случае имеют:

$$f(x, y) = f(x) + f(y) \text{ (то есть } f(x, y) = f(x) \otimes f(y)).$$

Этот односторонний сумматор обладает следующим свойством коммутативности (хотя для настоящего изобретения необходима только квазикоммутативность):

$$B = f(X) = x_1 \otimes x_2 \otimes x_3 \otimes \ldots \otimes x_\mu = x_1 \otimes (x_2 \otimes x_3 \otimes \ldots \otimes x_\mu) = x_2 \otimes (x_1 \otimes x_3 \otimes \ldots \otimes x_\mu),$$

и т.д.

А теперь X^i рассмотрим набор всех элементов X, за исключением x_i. Например, где i = 1, $X^1 = (x_2, x_3, \ldots x_\mu)$. Предполагая для простоты, что f(X) является коммутативной относительно элементов X, и учитывая свойство f(X) выше, это приводит к следующему:

$$B = f(X) = x_1 \otimes f(X^1) = f(X^1) \otimes x_1 = \left(x_2 \otimes x_3 \otimes \ldots \otimes x_\mu\right) \otimes x_1 = k_1 \otimes x_1$$

с ключом верификации

$$k_1 = \left(x_2 \otimes x_3 \otimes \ldots \otimes x_\mu\right) = f(X^1).$$

Согласно настоящему изобретению агрегированная цифровая подпись B партии изделий становится неизменной и, следовательно, защищенной от подделки, ввиду ее публикации в (общедоступной) среде, открытой для пользователя, который должен проверить аутентичность изделия (или связанных с ним данных), или ее хранения в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, или в предпочтительном варианте - ее хранения в блокчейне, открытом для пользователя. Затем пользователь может сохранить значение B, полученное из этих доступных источников.

Для каждого изделия A_i соответствующий ключ верификации изделия k_i затем вычисляют посредством частичного одностороннего сумматора других цифровых подписей изделий x_j (где $j \neq i$), то есть одностороннего сумматора цифровых подписей $x_1, \ldots x_{i-1}, x_{i+1} \ldots x_\mu$ или $f(X^i)$ Например, в модуле 120 согласно фиг. 1 ключ верификации k_i изделия A_i вычисляют как $k_i = f(X^i)$, и для операции проверки действительного соответствия цифровых данных изделия D_i и ключа верификации k_i изделия A_i данным подлинного изделия, принадлежащего к партии со значением партии B, необходима только верификация того, что $k_i \otimes f(H(D_i)) = B$, то есть $k_i \otimes x_i = B$. Полученный компактный (благодаря свойству сумматора) ключ верификации k_i, как часть информации о верификации $V_i = (D_i, k_i)$, необходимой для вычисления B, включен в защитную маркировку 110, нанесенную на изделие A_i вместе с цифровыми данными D_i изделия A_i. Это важный аспект настоящего изобретения, поскольку пространство, доступное для данных на защитной маркировке, обычно ограничено, в частности, для выполнения автономной проверки аутентичности защищенного изделия и автономной проверки соответствия связанных с ним данных относительно данных подлинного изделия. Тип одностороннего сумматора для f точно выбран с учетом технической задачи уменьшения размера данных ключа верификации, которые должны быть включены в защитную маркировку. Фактически, свойство квазикоммутативности (или даже коммутативности) таких сумматоров позволяет подписывать данные заданного изделия, принадлежащего к партии изделий, без необходимости дальнейшего включения данных, относящихся к упорядоченности изделий в партии или позиции указанного заданного изделия согласно упорядоченности в партии. Более того, без упомянутого свойства квазикоммутативности для операций верификации необходимо было бы гораздо большее количество компьютеров.

Модуль 120 вычисления предпочтительно включен в систему 100 защиты для выполнения кода, предусмотренного для выполнения вычислений для f(X), для значений ключа k_i для разных изделий, и для общего значения B. Система 100 защиты может также включать подходящие модули для ввода (запрограммированных) значений, соответствующих цифровым данным D_v виртуального изделия A_v. Хеширование цифровых данных D_i изделия A_i для получения соответствующей цифровой подписи изделия x_i можно также осуществлять, например, в модуле 120 вычисления. Также можно было бы осуществлять вычисления хеширования, связанные с изделиями, извне (например, на подключенном удаленном сервере), например, где бы ни изготовливались изделия, чтобы избежать необходимости передавать необработанные данные изделия D_i по сети с этого сайта (или сайтов) к системе 100 защиты, если есть проблема.

Для каждого изделия A_i компилируется соответствующая информация о верификации V_i, которая кодируется в некоторой форме машиночитаемой защитной маркировки 110, которая затем наносится физически или иным образом связывается с соответственным изделием. Например, V_i можно закодировать на оптически или магнитно читаемой этикетке, метке RFID и т.д., которая прикреплена к изделию или напечатана непосредственно на изделии или его упаковке. В качестве другого варианта маркировка может быть на внутренней стороне изделия или на его упаковке, если это необходимо, либо с использованием непосредственного нанесения, либо, например, путем включения в какую-либо форму документации, которая находится внутри упаковки.

Для любого "виртуального" изделия A_v его соответствующая информация о верификации V_v может быть связана с ним внутри системой 100 защиты. Информация о верификации, как правило, по меньшей мере включает, для любого изделия A_i партии изделий, соответствующие цифровые данные изделия D_i и соответствующий ключ верификации k_i: $V_i = (D_i, k_i)$. Согласно настоящему изобретению кодирование данных D_i и кодирование данных k_i могут отличаться (что обеспечивает дополнительный уровень надежности относительно криптоаналитических атак).

Дополнительные данные изделия могут дополнительно быть связаны с изделием и могут включать, например, значение партии B или любую другую информацию, которую разработчик системы выбирает включить, как, например, серийный номер товара, идентификатор партии, информация о дате/времени,

название продукта, URL-адрес, который указывает на другую онлайн-информацию, связанную либо с отдельным товаром (например, изображение изделия или его этикетки или упаковки и т. д.), либо с партией, либо с поставщиком/изготовителем, номером телефона, по которому можно позвонить для верификации и т. д. Дополнительные данные изделия могут храниться в доступной для поиска информационной базе данных, открытой для пользователя (посредством интерфейса информационной базы данных).

После вычисления верификации k_i оригинального изделия A_i и включения (то есть посредством кодирования или любого выбранного представления данных) вместе с соответствующими цифровыми данными изделия D_i в машиночитаемую защитную маркировку 110 изделия, нанесенную на изделие, полученное в результате маркированное оригинальное изделие и связанные с ним данные изделия действительно защищены от подделки и фальсификации. Преимущество настоящего изобретения состоит в том, что в защитную маркировку не включают ключ кодирования/декодирования.

Существуют различные типы физических (защитных) маркировок, которые можно использовать для кодирования ключа верификации и цифровых данных изделия (или любых других данных). Однако многие системы маркировки, которые можно использовать на практике на небольших товарах или на службах, которые не могут принимать физические маркировки с высоким разрешением, не могут кодировать большой объем данных. Одним из способов решения этой проблемы было бы включение нескольких маркировок, каждая из которых включает один или более элементов вектора верификации. Во многих случаях это непрактично из-за недостатка физического пространства или непригодности поверхности знака, или просто потому, что это было бы эстетически неприемлемо.

Существует множество известных методов кодирования информации, которые можно применить к физическим поверхностям. Любой такой метод можно использовать в реализациях любого варианта осуществления настоящего изобретения. Одной из распространенных форм физической маркировки является хорошо известный QR-код. Как хорошо известно, для заданной области, чем больше данных может кодировать QR-код, тем выше плотность модуля (грубо говоря, плотность черных/белых "квадратов") и тем большее разрешение требуется для печати и считывания. Помимо плотности (в количестве квадрата модулей), QR-коды также обычно классифицируются в зависимости от того, какой уровень исправления ошибок они включают. В настоящее время четыре разных стандартных "уровня", L, M, Q и H, каждый из которых представляет степень "повреждения", то есть потери данных, изображение QR-кода может выдержать и из которых может восстановиться. Уровни L, M, Q и H могут выдержать приблизительно 7%, 15%, 25% и 30% повреждения, соответственно. В следующей таблице приведены по меньшей мере приблизительные значения для разных версий QR-кода:

Версия	Размер (в модулях)	Количество кодируемых битов	
		уровень L ECC	уровень H ECC
10	57×57	2192	976
25	117×117	10208	4304
40	177×177	23648	10208

Однако, не все биты могут использоваться для кодирования "загрузки" данных, поскольку некоторые модули используются для объектов сканирования, шаблона маски и модулей исправления ошибок. Таким образом, существует компромисс между количеством информации, которую может кодировать QR-код (или любая другая маркировка 110), и тем, сколько информации включено в информацию о верификации V и должно быть закодировано.

Следовательно, для выбранного типа защитной маркировки 110 (например, QR-кода) с ограниченной способностью кодирования также должна быть выбрана подходящая функция кодирования f(X): функцию, выходные данные которой слишком велики с точки зрения требуемых битов, невозможно использовать вообще, а функция, диапазон которой слишком мал, может быть недостаточно надежной. Более того, во многих приложениях может возникнуть проблема с масштабируемостью. Например, некоторые схемы защиты данных включают подписи, которые растут по мере увеличения количества элементов партии, и которые могут недопустимо ограничивать размер партии с точки зрения того, сколько битов может кодировать защитная маркировка 110. Вот почему согласно настоящему изобретению выбран следующий тип функции - односторонний сумматор.

В одном иллюстративном варианте осуществления функция одностороннего сумматора f(X) выбрана как простое (коммутативное) умножение по модулю, то есть $f(x) = x \bmod m$, и $f(x, y) = x \otimes y = x * y \bmod m$.

Таким образом, в данном случае получают $f(x, y) = f(x) * f(y)$ и:

$$f(X) = \prod_{i=1}^{\mu} x_i \bmod m = \left(\prod_{i=1}^{\mu} x_i\right) \bmod m$$

то есть $f(X) = x_1 \otimes x_2 \otimes \ldots \otimes x_\mu$, где m представляет собой модуль, а X соответствует μ цифровых подписей μ изделий в партии $X = (x_1, \ldots, x_\mu)$. Умножение по модулю - это очень простой пример одностороннего сумматора (не только квази-коммутативного, но и коммутативного), хотя и не надежного. Таким образом, на словах значение партии $B = f(X)$ вычисляют путем умножения всех хеш-значений изделий x_i вместе, а затем взятия остатка данного произведения после деления на модуль m. В некоторых случаях это может привести к получению непрактично большого произведения. Например, предположим, что в партии 1000 изделий, и каждое хеш-значение xi имеет длину 256 бит (как получено с помощью хеш-функции SHA-256). Можно было бы выполнить 999 умножений и сохранить результат, а затем выполнить деление на m для получения остатка, но это неудобно и потребовало бы ненужных вычислительных усилий в виде сохранения значений без усечения. Вместо этого система может использовать свойство операций по модулю, что результат можно вычислять несколько раз, попарно, как показано в следующем псевдокоде:

B = 1
For j = 1 to μ
B := [B * x(j)] mod m
Следующее j.

Таким образом, значение B можно вычислять без необходимости умножения более двух хеш-значений перед определением произведения по модулю m.

Конечно, можно использовать любой другой метод для вычисления f(X) с использованием метода произведения по модулю m, показанного выше. Аналогичный алгоритм можно использовать для вычисления ключей верификации k_i - для вычисления ключа k_i просто нужно пропустить этап, на котором j=i.

Есть несколько преимуществ использования метода произведения по модулю m для определения значения партии B и ключей верификации. Одно из преимуществ состоит в том, что длина в битах не будет больше m, что может быть выбрано пользователем. Более того, вычисления не требуют операций с плавающей запятой, и, следовательно, не будет ошибок из-за усечения - стоит обратить внимание, что изменение одного бита в цифровой подписи изделия приведет к совершенно иному значению партии.

Выбор целочисленного модуля m также отражает компромисс между защитой и размером, как количества битов, которые может кодировать защитная маркировка 110, так и количества изделий в партии. Для иллюстрации рассмотрим очень упрощенный пример партии, который включает только три изделия, имеющие хеш-значения цифровых подписей x_1, x_2, x_3. Теперь предположим, что $m > \max(x_1, x_2, x_3)$, тогда:

$$x_1 \bmod m = x_1,$$

$$x_2 \bmod m = x_2, \text{ и}$$

$$x_3 \bmod m = x_3$$

Другими словами, при таком выборе m, нет защиты для отдельных значений H. С другой стороны, кроме тех случаев, когда m выбрано как $m >> \max(x_1, x_2, x_3)$, то маловероятно, что произведение любых двух хеш-значений по модулю m останется тем же значением, и еще менее вероятно, что будет произведение всех трех. Чем больше изделий и, следовательно, хеш-значений в партии, тем больше общее произведение будет "обтекать" модуль m (иметь ненулевой делитель) и тем сложнее будет использовать атаку "грубой силы", чтобы найти "поддельное" множимое (хеш-значение изделия), которое, умноженное на известное значение ключа, даст то же значение партии по модулю m. В качестве очень простого примера предположим, что x_1, x_2, x_3 и m равны 3, 6, 8 и 10.

$$3 \bmod 10 = 3,$$

$$6 \bmod 10 = 6, \text{ и}$$

$$8 \bmod 10 = 8$$

но

$$B = 3 \times 6 \times 8 \bmod 10 = 144 \bmod 10 = 4$$

Если ключ верификации для первого изделия задан как $6 \times 8 \bmod 10 = 8$, а значение партии B = 4, чтобы угадать хеш-значение 3 изделий, все равно нужно будет угадать набор из десяти возможностей. Сложность, конечно, будет расти по мере увеличения длины в битах x_i и m. Специально для партий из

более чем десяти изделий или более 100 изделий, где m установлено в виде $m > \max_i(x_i)$, например, до максимального значения, которое может быть представлено для заданной длины в битах (такой как 256 для реализации, которая использует хеш-функцию SHA-256), злоумышленнику будет неэффективно пытаться вычислительным образом подделать хеш-значение для каждой подписи партии изделий, особенно в реализациях, в которых финансовая ценность каждого изделия в партии слишком мала, чтобы оправдать попытку такой атаки. Другими словами, используя этот вариант осуществления, нет смысла пытаться подделать информацию, закодированную в маркировке.

Преимущество $m > \max(x_1, x_2, ... x_\mu)$ выбора состоит в том, что для всех хеш-значений ($x_i \bmod m = x_i$) существует свойство эквивалентности, но это не обязательно. Скорее, может быть выбрано любое значение, в частности, для обеспечения желаемой длины в битах для B. Также необязательно, чтобы m было постоянным во всех реализациях настоящего изобретения или даже для всех партий. В качестве одного из примеров администратор, изготовитель и т.д. может выбрать разный модуль m для разных партий. Они могут храниться в базе данных либо в системе 100 защиты, либо где-либо еще, либо доставляться через какой-либо другой канал пользователю, например, получателю изделий, чтобы только этот получатель мог легко верифицировать изделия на основании их защитной маркировки 110.

Чтобы избежать необходимости поддерживать значения модуля в базе данных, также можно было бы вычислить сам m для каждой партии, например, как функцию хеш-значений x_i. В качестве всего лишь одного примера, m может быть выбран в виде $m = [\max(x_1, x_2, ... x_\mu)] + 1$. Затем модуль 120 может определить модуль m перед осуществлением других вычислений, как, например, f(X), k_i и B. Модуль 120 может также ввести выбранный пользователем размер кодирования (например, версию QR-кода) и определить пригодный модуль (и, следовательно, размер в битах), чтобы гарантировать, что закодированные данные (D_i, k_i) в защитной маркировке будут совпадать, то есть данные, необходимые для извлечения $x_i = H(D_i)$ и вычисления значения партии B из:

$$f(x_i \otimes X^i) = x_i \otimes f(X^i) = f(X^i) \otimes x_i = k_i \otimes x_i.$$

Пользователь, получатель изделия, такого как A_1, например, может затем сканировать (или иным образом считывать) с помощью устройства для формирования изображения защитную маркировку на A_1 и извлекать цифровые данные изделия D_1 и ключ верификации k_1 (и любую другую информацию, которая могла быть закодирована в маркировке). Для верификации маркированного изделия A_1 пользователь должен сначала извлечь информацию о верификации $V_1=(D_1, k_1)$ из защитной маркировки на A_1 и, таким образом, вычислить цифровую подпись x_1 из извлеченных цифровых данных изделия D_1: чтобы выполнить такую операцию, пользователь должен знать одностороннюю функцию, которая используется для вычисления цифровой подписи изделия, в данном случае это хеш-функция H(), а затем выполнить операцию $x_1 = H(D_1)$ для получения полных данных (x_1, k_1), необходимых для вычисления соответствующей потенциальной агрегированной цифровой подписи B^c. Пользователь может, например, безопасно принять одностороннюю функцию (например, используя пару открытого и личного ключей) или запросив ее у поставщика изделий или любого другого объекта, который создал подписи и ключи или уже запрограммировал их в блок обработки устройства для формирования изображения пользователя.

Затем, чтобы вычислить такую потенциальную агрегированную цифровую подпись B^c, пользователю необходимо дополнительно знать тип одностороннего сумматора f(), который будет использоваться для этого, в данном случае пользователю необходимо знать модуль m умножения по модулю (или аналогичную информацию при использовании некоторой другой функции f). Предполагая, что "стандартный" модуль не используется, например, для всех изделий от поставщика, пользователь может затем принять модуль любым известным способом, либо безопасно (например, используя пару открытого и личного ключей), либо просто запрашивая это у поставщика изделий или любого другого объекта, который создал данные верификации или уже запрограммировал их в блоке обработки пользователя.

Используя модуль m, пользователь может затем вычислить потенциальную агрегированную цифровую подпись $B^c = k_1 \otimes x_1$, которая затем должна быть равна доступному (или опубликованному) значению B: это значение могло быть ранее получено пользователем и/или уже сохранено в памяти блока обработки устройства для формирования изображения, это также может быть значение, которое получатель запрашивает и принимает от системного администратора любым известным способом. При совпадении потенциальных B^c и доступных агрегированных цифровых подписей B данное вычисление затем верифицирует информацию в защитной маркировке 110 и подтверждает, что изделие A_1 принадлежит правильной партии. Защитную маркировку предпочтительно предусматривать и/или наносить на изделие любым трудным для копирования и/или трудным для удаления (защищенным от несанкционированного доступа) способом. В этом случае совпадение агрегированных цифровых подписей может указать пользователю, что изделие, вероятно, является подлинным. Это особенно интересно, потому что для аутентификации изделия A_1 нет необходимости в аутентификации его материала, то есть посредством внутренней физической характеристики A_1 или посредством защитной маркировки на основе материала, нанесенной на A_1.

Ссылка для доступа к значению партии B для партии, соответствующему изделию A_1, может быть включена в защитную маркировку 110 (например, веб-адрес, если B можно извлечь из соответствующего

веб-сайта), хотя это не предпочтительный вариант.

В некоторых реализациях получатели изделия A_1 могут иметь возможность "визуально" извлекать данные изделия, соответствующие цифровым данным изделия D_1, непосредственно из изделия. Например, данные изделия могут быть текстовыми, такими как серийный номер или текст в описательном письме, или являться некоторым буквенно-цифровым кодированием в другом месте на изделии или его упаковке и читаться человеком из самих изделий или чего-либо, прикрепленного к ним или включенного в них. Получателям изделий также может быть предоставлено пригодное программное обеспечение, такое как модуль в устройстве для формирования изображения, таком как смартфон, который либо вводит данные, либо считывает данные оптически через камеру телефона, а затем вычисляет $x_i = H(D_i)$ для текущего изделия. Например, с помощью защитной маркировки 110 на изделии A_1, представляющей собой стандартный QR-код, пользователь сможет легко получить путем сканирования QR-кода с помощью устройства для формирования изображения, используя стандартное приложение для считывания QR-кода, запущенное на устройстве для формирования изображения, цифровые данные D_1 и k_1, приложение для верификации на устройстве для формирования изображения пользователя затем сможет вычислить $x_1 = H(D_1))$ и $B^c = f(X) = f(x_1 \otimes X^1) = x_1 \otimes f(X^1) = f(X^1) \otimes x_1 = k_1 \otimes x_1$, а также сравнить данное значение с доступным значением партии B, как раскрыто выше. Например, если оператор $\otimes$ соответствует умножению по модулю, то $k_1 \otimes x_1 = (k_1 * x_1) \bmod m$.

Предпочтительно, агрегированная цифровая подпись (то есть значение партии) B хранится в доступной для поиска базе данных агрегированных подписей, к которой может получить доступ (через канал связи) пользователь с помощью своего устройства для формирования изображения, оснащенного устройством для связи, как это имеет место с приведенным выше примером смартфона. Пользователь, которому необходимо верифицировать изделие A_1, может просто отправить запрос со своего смартфона на адрес базы данных через интерфейс сбора подписей базы данных, запрос, содержащий данные изделия D_1, считанные на защитной маркировке 110, на A_1 (или вычисленную цифровую подпись $x_1 = H(D_1))$, что позволяет извлечь соответствующее значение партии B, а интерфейс сбора данных вернет агрегированную цифровую подпись B на смартфон. База данных может быть защищена блокчейном, чтобы усилить неизменность сохраненных агрегированных подписей. Преимущество настоящего изобретения заключается в том, чтобы установить связь между физическим объектом, то есть оригинальным изделием и его атрибутами, то есть связанными данными изделия и его принадлежностью к партии изделий, практически неизменно посредством соответствующей агрегированной цифровой подписи.

Вышеупомянутый способ верификации изделия A_i может также служить для аутентификации читаемых человеком данных изделия, дополнительно маркированных на A_i на соответствующей маркировке данных изделия, нанесенной на A_i или напечатанной на упаковке A_i или на брошюре. Действительно, пользователь может считать на дисплее устройства для формирования изображения соответствующие цифровые данные изделия D_i как считанные на защитной маркировке на изделии A_i и декодированные устройством для формирования изображения, и визуально проверить, соответствует ли отображаемая информация данным изделия на маркировке данных изделия.

В предпочтительном варианте осуществления данные изделия или его соответствующие цифровые данные изделия D_i дополнительно включают данные уникальной физической подписи уникальной физической характеристики маркированного оригинального изделия A_i, что можно использовать для (материальной) аутентификации A_i. Таким образом, с помощью цифровых данных, соответствующих уникальной физической характеристике изделия A_i, представляющих собой UPC_i, соответствующие данные уникальной физической подписи UPS_i можно получить путем кодирования UPC_i (предпочтительно посредством односторонней функции): например, взяв хеш-значение цифровых данных UPC_i, то есть $UPS_i = H(UPC_i)$. Однако, вместо этого можно использовать любое другое известное кодирование: например, чтобы иметь короткую подпись, можно использовать алгоритм цифровой подписи эллиптической кривой. В качестве очень упрощенного иллюстративного примера цифровых данных UPC_i соответствующих уникальной физической характеристике изделия A_i, рассмотрим простое цифровое изображение, полученное отображением изделия A_i (или конкретной зоны на A_i), при этом соответствующие данные уникальной физической подписи UPS_i представляют собой, например, хеш-значение цифрового изображения, $UPS_i = H(UPC_i)$. Цифровые данные UPC_i, которые генерировали подпись UPS_i, представляют собой контрольные физические характеристические цифровые данные для A_i, и полученная подпись UPS_i представляет собой соответствующие контрольные данные физической подписи для A_i. Предпочтительно, UPS_i, то есть контрольные данные физической подписи для изделия A_i, хранятся в доступной для поиска базе данных или в блокчейне (или в базе данных, защищенной блокчейном), открытых для пользователей (например, посредством запроса, содержащего цифровые данные изделия D_i, считываемые на защитной маркировке A_i, или их соответствующую цифровую подпись x_i). Таким образом, сохраненная UPS_i приобретает неизменный характер. Копия UPC_i может дополнительно храниться в памяти устройства для формирования изображения пользователя. В варианте осуществления копию UPS_i можно также дополнительно хранить в памяти устройства для формирования изображения пользователя (для обеспечения операции автономной проверки).

Проверку аутентичности изделия A_i можно осуществлять путем извлечения потенциальных цифровых данных уникальной физической характеристики UPC_i^c из цифровых данных D_i, считываемых (в данном случае с помощью приложения для декодирования, запущенного на устройстве для формирования изображения, которое может представлять собой, например, смартфон)) на защитной маркировке на изделии A_i, и сравнения их с контрольными цифровыми данными уникальной физической характеристики UPC_i, сохраненными в памяти устройства для формирования изображения: в случае совпадения $UPC_i^c = UPC_i$, изделие A_i считается подлинным (его цифровое содержимое соответствует содержимому подлинного маркированного оригинального изделия). Если контрольные цифровые данные уникальной физической характеристики UPC_i не хранятся в памяти устройства для формирования изображения, а напротив, контрольные данные уникальной физической подписи UPS_i хранятся в памяти устройства для формирования изображения (с тем преимуществом, что они занимают гораздо меньше памяти по сравнению с UPC_i), то аутентичность A_i все еще можно проверять путем верификации того, что потенциальные данные уникальной физической подписи UPS_i^c, получаемые путем вычисления хеш-значения потенциальных цифровых данных уникальной физической характеристики UPC_i^c, извлеченных из цифровых данных D_i, то есть $UPS_i^c = H(UPC_i^c)$, совпадают с контрольными данными уникальной физической подписи UPS_i, сохраненными в памяти.

Пользователь может дополнительно проверить аутентичность принятого изделия A_i все еще посредством автономного процесса (самоконтроль), путем обнаружения указанной уникальной физической характеристики на A_i, посредством датчика, выполненного с возможностью осуществления такого измерения (в данном случае блока формирования изображения устройства для формирования изображения), и получения потенциальных цифровых данных уникальной физической характеристики UPC_i^c из обнаруженной характеристики (в данном случае цифрового изображения, снятого устройством для формирования изображения). Таким образом, пользователь может сравнивать (посредством блока обработки изображения его устройства для формирования изображения, или визуально на дисплее устройства для формирования изображения) полученные UPC_i^c с копией контрольных UPS_i (сохраненных в памяти устройства для формирования изображения): в случае "обоснованного" совпадения $UPC_i^c \approx UPC_i$ (то есть два цифровых данных согласуются с неким заданным критерием отклонения или схожести), изделие A_i считается подлинным.

Более того, пользователь может также дополнительно вычислить соответствующие потенциальные данные физической подписи из копии контрольных UPC_i, сохраненных в памяти устройства для формирования изображения в виде $UPS_i^c = H(UPC_i)$, и сравнить их с контрольными данными физической подписи UPS_i, сохраненными в памяти устройства для формирования изображения: в случае совпадения $UPS_i^c = UPS_i$, подтверждается, что изделие A_i является подлинным с более высокой степенью достоверности. Более того, в случае совпадения, также устанавливают аутентичность цифровых данных изделия D_i, связанных с A_i, которые были верифицированы как соответствующие данным подлинного изделия, как раскрыто выше, путем извлечения соответствующего значения партии B из считанной информации о верификации (D_i, k_i) на защитной маркировке на A_i. В предпочтительном режиме копия контрольных физических характеристических цифровых данных UPC_i, вместо того, чтобы храниться в памяти устройства для формирования изображения пользователя, является частью цифровых данных изделия D_i, включенных в защитную маркировку на изделии A_i, и может быть получена путем ее считывания на защитной маркировке (с помощью устройства для формирования изображения). Однако в варианте (все еще совместимом с автономной верификацией) копия контрольных физических характеристических цифровых данных UPC_i может, вместо этого, быть включена в маркировку данных изделия, нанесенную на изделие A_i (и считываемую устройством для формирования изображения пользователя).

В варианте осуществления проверку аутентичности изделия A_i пользователем можно осуществлять посредством процесса в режиме "онлайн": в данном случае, контрольные данные UPCi и/или UPSi хранятся в доступной для поиска базе данных, открытой для пользователя, при этом контрольные данные, относящиеся к изделию A_i, хранятся в связи с, соответственно, соответствующими цифровыми данными изделия D_i (включенными в защитную маркировку на A_i) или с соответствующей цифровой подписью изделия x_i (которую можно вычислить пользователем при извлечении данных D_i из защитной маркировки посредством операции $x_i = H(D_i)$ и можно запросить путем отправки в базу данных запроса, содержащего, соответственно, D_i или x_i.

Конечно, любое другое известное внутреннее физическое/химическое свойство можно использовать для получения цифровой уникальной физической характеристики UPC_i изделия A_i и соответствующих данных уникальной физической подписи UPS_i. В качестве другого иллюстративного примера можно напечатать двухмерный штрих-код, образующий защитную маркировку 110 на оригинальном изделии с помощью защитной краски, содержащей люминесцентный пигмент, имеющий характеристическую постоянную времени затухания, а также окно длины волны возбуждения света и окно длины волны люминесцентного испускания: в результате краска имеет определенное контрольное значение времени затухания τ, которое служит "отпечатком пальца" материала краски. Достаточно осветить защитную маркировку 110 возбуждающим светом в окне длины волны освещения, охватывающем окно длины волны возбу-

ждения пигмента, и собрать полученный в результате люминесцентный свет с защитной маркировки с помощью датчика, выполненного с возможностью определения интенсивности света в пределах окна длины волны люминесцентного испускания, чтобы аутентифицировать защитную маркировку. Например, устройство для формирования изображения пользователя может быть оснащено вспышкой, выполненной с возможностью подачи возбуждающего света на защитную маркировку, фотодиодом, выполненным с возможностью сбора соответствующего профиля интенсивности люминесцентного света I(t) (в течение интервала времени обнаружения) с защитной маркировки, и ЦП устройства для формирования изображения, запрограммированным для вычисления значения времени затухания на основе полученного профиля интенсивности I(t). Например, окно длины волны возбуждения может находиться в УФ (ультрафиолетовом) диапазоне, а окно длины волны испускания - в ИК (инфракрасном) диапазоне. Если во время верификации изделия интенсивность люминесцентного света, собираемая устройством для формирования изображения пользователя, показывает характеристическое затухание с течением времени, соответствующее потенциальному времени затухания τ_c, то краска и, следовательно, защитная маркировка считаются подлинными, если $\tau_c \neq \tau$ (в заданном диапазоне отклонения). В данном случае цифровые данные UPC_i маркированного изделия A_i включают по меньшей мере контрольное значение τ времени затухания (и, возможно, данные, относящиеся к окну длины волны возбуждения и окну длины волны испускания). Как видно из приведенных выше примеров, технический результат включения контрольных цифровых данных уникальной физической характеристики в информацию о верификации защитной маркировки заключается в обеспечении защищенной от подделки связи между цифровыми данными изделия и данными аутентификации этого конкретного изделия.

Вместо произведения по модулю m в приведенном выше иллюстративном примере можно использовать любой другой известный (коммутативный или квази-коммутативный) односторонний сумматор (с соответствующим ему оператором ⊗). Например, квази-коммутативный односторонний сумматор, определяемый $f(x) = f(I; x) = I^x \bmod m$ (то есть возведение в степень по модулю m) или эквивалентной символической записью оператора $I \otimes x$, где I - заданное число (целое число), а m - заданный модуль. Таким образом, $f(x, y) = f(I; x, y) = f(f(I; x), y) = f(I; x) \otimes y = (I^x \bmod m)^y \bmod m = I^{x*y} \bmod m = I \otimes x * y$. Агрегированную цифровую подпись B для партии μ изделий A_1, A_2 .... A_μ (что может включать виртуальные изделия), соответственные цифровые данные изделия которых представляют собой D_1, D_2 .... D_μ, с соответствующими связанными с изделиями цифровыми подписями x_1, x_2 ....x_μ, вычисляют для $X = (x_1, x_2 \ldots .x_\mu)$, как $B = f(I; X)$, то есть:

$$B = f(f(f(\ldots f(f(f(I, x_1), x_2), x_3), \ldots, x_{\mu-2}), x_{\mu-1}), x_\mu),$$

что можно уменьшить, на основании квази-коммутативности f, к:

$$B = f(X) \equiv f(I; X) = \left(I^{\prod x_i}\right) \bmod m = I \otimes \prod x_i,$$

где $\prod x_i$ обозначает произведение от i=1 до i=μ компонентов цифровых подписей изделия x_1, x_2, ... x_μ X, то есть $\prod x_i = x_1 * x_2 * \ldots * x_\mu$. Действительно, квази-коммутативность этого одностороннего сумматора позволяет записать (для всех I и всех x, y): f(f(I;x),y) = f(f(I;y),x), где вышеупомянутое полученное в результате преимущество заключается в том, что этап верификации не требует наличия дополнительной информации о упорядоченности подписей x_i.

Вычисляют цифровые подписи изделий x_i, как раскрыто выше, посредством любой известной односторонней функции. Предпочтительно, цифровую подпись x_i получают посредством хеш-функции соответствующих цифровых данных изделия D_i: $x_i = H(D_i)$ (для вышеупомянутых причин).

Ключ верификации kj, соответствующий цифровой подписи x_i цифровых данных D_j изделия A_j из партии □ изделий, вычисляют следующим образом: $k_j = I(\prod xi/xj) \bmod m$, где $(\prod x_i/x_j) = x_1 * x_2 * \ldots * x_{j-x} * x_{j+1} \ldots * x_\mu$, или где символическое обозначение $k_j = I \otimes x_1 * x_2 * \ldots * x_{j-x} * x_{j+1} \ldots * x_\mu$.

Если обозначение $X^j = (x_1 * x_2 * \ldots * X_{j-1} * X_{j+1} \ldots * x_\mu)$, получают более компактную формулу $k_j = f(X^j)$, где $(\prod x_i/x_j) = x_1 * x_2 * \ldots * x_{j-1} * x_{j+1} \ldots * x_\mu$ представляет собой произведение компонентов X^j.

Следовательно, для операции проверки действительного соответствия цифровых данных изделия D_j и ключа верификации k_j из защитной маркировки изделия A_j данным подлинного изделия, принадлежащего к партии, имеющей значение партии B, необходимо только вычисление цифровой подписи изделия x_j в виде $x_j = H(D_j)$, а затем верификация того, что x_j и k_j обеспечивают извлечение агрегированной цифровой подписи B посредством:

$$k_j^{H(D_j)} \bmod m = k_j^{x_j} \bmod m = B \ (\text{or } k_j \otimes x_j = B).$$

Предпочтительно (целочисленный) модуль m выбирается таким, чтобы он имел размер по меньшей мере 2048 бит, чтобы обеспечить хорошую устойчивость относительно криптоаналитических атак.

Вышеупомянутый оператор возведения в степень (и все его известные "варианты", такие как оператор Naccache $f(x) = I^x C^{x-1} \bmod m$, например, для любых заданных чисел I и C) - это просто еще один пример одностороннего сумматора, приведенный в данном случае для иллюстративных неограничивающих целей.

Другой иллюстративный вариант осуществления настоящего изобретения относится к партии биометрических идентификационных документов, например, биометрические паспорта, как показано на фиг. 2.

В этом примере по-прежнему используют хеш-функцию как одностороннюю функцию для подписывания данных паспорта, предпочтительно хеш-функцию SHA-256 ввиду ее хорошо известной надежности. Действительно, с учетом заданного размера партии, хэш-функция, которая выбрана (имеющая известный список сегментов) для подписания данных паспорта, является, таким образом, примером односторонней функции шифрования, так что каждый отдельный паспорт имеет отдельную подпись паспорта, что делает подпись уникальной. Домен хеш-функции (то есть набор возможных ключей) больше, чем ее диапазон (то есть количество различных индексов таблицы), он будет отображать несколько разных ключей в один и тот же индекс, что может привести к конфликтам: таких конфликтов можно избежать, когда размер партии известен, путем рассмотрения списка сегментов, связанного с хеш-таблицей хеш-функции, и сохранения только функции, дающей нулевые конфликты, или путем независимого выбора схемы разрешения конфликтов хеш-таблицы (например, такой как coalesced hashing, cuckoo hashing или hopscotch hashing).

На фиг. 2A показан пример биометрического паспорта A_1, защищенного машиночитаемой защитной маркировкой 210 (в данном случае QR-кодом), и содержащего маркировку 230 данных паспорта, содержащую обычные данные паспорта, то есть видимые напечатанные данные, такие как название документа 230a ("Паспорт"), набор биографических данных владельца паспорта 230b: фамилия ("Доу"), имя ("Джон"), пол ("М"), дата рождения ("20 марта 1975 г."), гражданство ("США"), место проживания ("Де-Мойн"), место рождения ("Окленд"), дата 230c выдачи ("24 февраля 2018 г.") и дата окончания срока действия 230d ("23 февраля 2020 г."). Эти данные паспорта могут дополнительно содержать некоторый(е) (уникальный(е)) серийный(е) номер(а) 235, присвоенный(е) органом, выдающим паспорт (в данном случае "12345").

Данные паспорта дополнительно содержат биометрические данные владельца паспорта в виде данных, соответствующих уникальной физической характеристике (UPC) человека, связанного с паспортом. Машиночитаемое представление 230e (например, буквенно-цифровое) данных, характеризующих указанную уникальную физическую характеристику (не показана), соответствующую указанным биометрическим данным, связано с данными 230 паспорта. Представление цифровых данных следует понимать в широком смысле этого термина: для этого представления данных необходимо только обеспечение извлечения оригинальных цифровых данных. Машиночитаемое представление 230e данных, то есть биометрические данные, уникальной физической характеристики, может соответствовать, например, идентификационным данным отпечатка пальца или идентификационным данным радужной оболочки глаза владельца паспорта. Например, биометрические данные 230e, соответствующие отпечатку пальца человека, могут быть результатом анализа набора конкретных мелких особенностей выступов отпечатка пальца, таких как окончание гребня, бифуркация и короткие гребни (согласно традиционной системе классификации Генри).

Таким образом, для заданного паспорта A_j из партии μ доставленных биометрических паспортов, в данном случае где $\mu = 1024$, связанные цифровые данные D_j паспорта включают цифровые данные, соответствующие вышеупомянутым данным 230a-230e. Предпочтительно, дополнительные цифровые данные паспорта связаны с вышеупомянутыми данными 230 паспорта. Например, цифровое изображение рисунка отпечатка пальца владельца паспорта или цифровая фотография, удостоверяющая личность, и т. д. В варианте осуществления эти дополнительные цифровые данные паспорта хранятся в доступной для поиска информационной базе 250 данных, в которой можно выполнять поиск с помощью запроса на информацию, содержащего некоторые данные паспорта (например, имя владельца, или биометрические данные, или данные из защитной маркировки, или уникальный серийный номер 235) для извлечения соответствующих данных рисунка отпечатка пальца и приема их обратно. Предпочтительно, чтобы ссылка на информационную базу 250 данных была включена в маркировку 240 по доступу к информации, нанесенную на паспорт: в данном случае она представляет собой QR-код, содержащий ссылочный индекс для извлечения соответствующих дополнительных данных в информационной базе 250 данных. Однако, в варианте операции паспортного контроля, включающей доступ к удаленной информационной базе данных (операция в режиме "онлайн"), QR-код может содержать, например, URL-адрес информационной базы данных, доступной через Интернет.

Цифровую подпись с помощью односторонней хэш-функции цифровых данных паспорта D_j, соответствующих данным 230a-230e паспорта A_j, затем вычисляют посредством, например, вышеупомянутой надежной хеш-функции SHA-256 для получения соответствующей (уникальной) цифровой подписи паспорта $x_j = H(D_j)$. Таким же образом вычисляют цифровые подписи всех паспортов в партии для всех различных владельцев.

На основе всех подписей паспортов в партии вычисляют агрегированную цифровую подпись B с помощью одностороннего сумматора. Например, в этом варианте осуществления агрегированную подпись для партии получают посредством вышеупомянутого одностороннего сумматора возведения в сте-

пень по модулю m, определяемого $f(x) = I^x \bmod m$, где I - заданное целое число, а m - модуль. Таким образом, агрегированную цифровую подпись B для партии μ биометрических паспортов A_1, A_2 .... A_μ (которая может включать виртуальные паспорта), соответствующие цифровые данные паспорта которого представляют собой D_1, D_2 .... D_μ, ис соответствующими связанными с паспортами цифровыми подписями $x_1 = H(D_1)$, $x_2 = H(D_2)$, ..., $x_\mu = H(D_\mu)$, вычисляют для $X = (x_1, x_2, ..., x_\mu)$, как;

$$B = f(X) = \left(I^{\prod x_i}\right) \bmod m,$$

где $\prod x_i$, обозначает произведение от i=1 до i=μ цифровых подписей паспорта x_1, x_2, x_μ, то есть $\prod X_i = x_1 * x_2 * ... * x_\mu$, и размер модуля m выбран таким образом, чтобы составлять, например, 2048 битов. Как раскрыто выше, при обозначении $X^j = (x_1, x_2, ... * x_{j-1}, x_{j+1}, ..., x_\mu)$, ключ верификации k_j для паспорта A_j вычисляют как частичный односторонний сумматор $k_j = f(X^j)$, и информацию о верификации (D_j, K_j) включают в защитную маркировку 210, нанесенную на паспорт A_j. Для операции проверки действительного соответствия цифровых данных паспорта D_j и ключа верификации k_j биометрического паспорта A_j данным подлинного биометрического паспорта, принадлежащего к партии биометрических паспортов, имеющей значение партии B, необходимо только вычисление цифровой подписи паспорта $x_j = H(D_j)$ и верификация того, что x_j и ключ верификации k_j обеспечивают извлечение доступного соответствующего значения партии B посредством: $k_j^{Xj} \bmod m = B$ (или $k_j \otimes x_j = B$). Таким образом, биометрический паспорт, защищенный согласно настоящему изобретению, обеспечивает как защищенную от подделки связь между "личными данными" и "биометрическими данными" его владельца, так и уникальную и защищенную от подделки связь между физическим лицом владельца и личностью владельца.

На фиг. 2B проиллюстрирован процесс контроля защищенного биометрического паспорта A_1 согласно фиг. 2A, в котором маркировка 230 данных паспорта соответствует конкретному Джону Доу, биометрические данные 230e паспорта соответствуют отпечатку пальца Джона Доу, и дополнительные цифровые данные паспорта соответствуют цифровой фотографии 255 личности Джона Доу, которая доступна посредством ссылки в информационную базу 250 данных, включенную в маркировку 240 по доступу к информации. Данные паспорта дополнительно содержат уникальный серийный номер 235, присвоенный органом, выдающим паспорт. Защитная маркировка 210, нанесенная на паспорт, содержит информацию о верификации (D_1, k_1), в которой цифровые данные паспорта D_x соответствуют напечатанным данным 230a-230d паспорта, биометрическим данным 230e и уникальному серийному номеру 235, и ключ верификации k_1 соответствует $f(X^1)$, при обозначении $X^1 = (x_2, ..., x_{1024})$, $x_i = H(D_i)$ i = 2, ..., 1024 и f представляет собой возведение в степень по модулю m (с заданными значениями целых чисел I и m). Значение партии B получают из всех цифровых подписей паспорта (x_1; ...,x_{1024}) как B = f(X), где ($X = x_1$, ..., x_{1024}). Вычисленной агрегированной цифровой подписи B можно дополнительно присваивать временную метку и хранить ее в блокчейне 260. В данном примере биометрические данные 230e соответствующих владельцев биометрических паспортов партии также хранятся в блокчейне 260 в связи с, соответственно, их соответствующими уникальными серийными номерами (чтобы обеспечить неизменность этих данных). Сохраненные биометрические данные Джона Доу можно извлечь, отправив запрос в блокчейн 260 с указанием уникального серийного номера 235, указанного в его паспорте. Органы, ответственные за контроль личности людей (например, полиция, таможня и т. д.), могут получить доступ к блокчейну 260 через канал связи и в этом иллюстративном варианте осуществления также имеют локальные хранилища для хранения (опубликованных) агрегированных цифровых подписей всех доставленных партий биометрических паспортов. В примере, показанном на фиг. 2B, информационная база 250 данных является локальной (то есть непосредственно доступна органам, без необходимости использования общедоступной сети связи). Кроме того, эти органы оснащены сканерами 270 отпечатков пальцев для захвата отпечатков пальцев людей и вычисления соответствующих машиночитаемых представлений данных, характеризующих снятые отпечатки пальцев, то есть биометрические данные 230e.

Во время проверки личности Джона Доу, скажем, сотрудником полиции или таможни, сотрудник берет защищенный биометрический паспорт A_1 Джона Доу, считывает и декодирует информацию о верификации (D_1, k_1), сохраненную в защитной маркировке 210 на паспорте, посредством пригодного портативного считывателя 280, подключенного к компьютеру 290 (образующих устройство для формирования изображения), при этом компьютер подключен к локальным хранилищам 250. После считывания цифровых данных паспорта D_1 и ключа верификации k_1 и отправки их на компьютер 290, определенное приложение (с запрограммированной хеш-функцией H и односторонним сумматором), запущенное на компьютере 290, вычисляет цифровую подпись паспорта x_1 (как $x_1 = H(D_1)$) и потенциальное значение партии B^c как $k_1^{X1} \bmod m = B^c$. Затем компьютер может, например, выполнить поиск в локальной информационной базе 250 данных значения партии B, соответствующего значению B^c: в случае несовпадения паспорт является поддельным и "Джон Доу" (то есть проверяемый человек, утверждающий, что его зовут Джон Доу) может быть арестован. В случае совпадения B^c с некоторым сохраненным значением партии B, паспорт считается подлинным, и сотрудник может выполнить дополнительные проверки безопасности: сотрудник извлекает цифровую фотографию 255 личности, хранящуюся в информационной базе 250 данных, путем отправки запроса через компьютер 290, содержащего серийный номер 235, напечатанный на A_1, принимает его обратно и отображает принятую фотографию 255 личности на экране компьютера

290: затем сотрудник может визуально сравнить отображаемое лицо (то есть лицо Джона Доу) с лицом проверяемого человека и оценить, похожи ли эти два лица или нет; и сотрудник извлекает биометрические данные 230e в паспорте A_1 путем считывания этих данных на защитной маркировке 210 с помощью портативного считывателя 280, подключенного к компьютеру 290, и сканирует отпечаток пальца человека с помощью сканера 270 отпечатков пальцев, подключенного к компьютеру 290, и получает биометрические данные соответствующего человека: сотрудник затем проверяет посредством программы, запущенной на компьютере 290, сходны ли извлеченные биометрические данные 230e (в пределах заданной погрешности) с полученными биометрическими данными человека.

Если два лица и биометрические данные считаются одинаковыми, все в порядке, и проверяемый человек действительно является Джоном Доу, владельцем подлинного биометрического паспорта A_1.

В случае неудачной попытки какой-либо из вышеупомянутых дополнительных проверок безопасности очевидно, что человек перед сотрудником не является истинным владельцем подлинного биометрического паспорта A_1 и, вероятно, украл паспорт некоего Джона Доу. Таким образом, с помощью защищенного биометрического паспорта согласно настоящему изобретению простая автономная проверка может быстро обнаружить любое мошенничество.

Фактически, можно даже уменьшить биометрический паспортный документ до простого кусочка бумаги с просто напечатанным двухмерным штрих-кодом (как в вышеупомянутом примере QR-кода), включающим информацию о верификации V = (D, k): с V, содержащим биографические данные владельца и (уникальные) биометрические данные, такие как отпечаток пальца владельца (в цифровых данных D паспорта) и ключ верификации. В действительности, согласно настоящему изобретению даже этот "уменьшенный" защищенный паспорт имеет полное преимущество вышеупомянутой защищенной от подделки связи, созданной между "личными биографическими данными" и "биометрическим данными" владельца паспорта и уникальной и защищенной от подделки связи между физическим лицом владельца и личностью владельца.

Другой иллюстративный вариант осуществления настоящего изобретения относится к компонентам самолета, как показано на фиг. 3. Из-за очень высокой стоимости некоторых критически важных компонентов, отказ которых может повлиять на безопасность самолета, таких как некоторые детали реакторов (например, лопатки турбины, насосы и т. д.) или шасси, или батареи и т.д., фальсификаторы заинтересованы производить копии этих компонентов, но, конечно, без соблюдения необходимых технических требований безопасности ввиду их, как правило, более низкого качества. Даже если компонент самолета обычно маркируется соответствующим уникальным серийным номером для его идентификации, такого рода маркировка может быть легко подделана. Эти поддельные детали самолета, как правило, имеют дефекты и могут вызвать серьезные повреждения или даже авиакатастрофы. Сегодня это растущая проблема безопасности. Более того, даже если компоненты являются подлинными, они могут быть неподходящими для определенных версий одного и того же типа самолета, и существует серьезный риск того, что непригодный компонент будет случайно использован, например, для ремонта данного самолета. Таким образом, важно обеспечить, по меньшей мере, критически важные подлинные компоненты, которые разрешены для данного самолета.

Как правило, каждый компонент имеет соответствующий технический паспорт с указанием, например, технического названия компонента, уникального серийного номера компонента, названия изготовителя компонента, даты изготовления компонента и информации о сертификации. Более того, для данного самолета соответствующая запись содержит все технические паспорта его соответствующих компонентов. Тем не менее, поддельные компоненты могут иметь соответствующий поддельный технический паспорт, и поэтому не очевидно (если только, например, не проводить технические испытания) выявить мошенничество. Например, как быть уверенным, что технический паспорт правильно соответствует компоненту, установленному на конкретном самолете (и наоборот)?

Согласно иллюстративному варианту осуществления настоящего изобретения разрешенные части, которые будут использоваться для производства или ремонта данного самолета или которые установлены на самолете, считаются принадлежащими к партии "изделий" для этого конкретного самолета.

В конкретном иллюстративном варианте осуществления, показанном на фиг. 3, каждое изделие партии самолета, то есть каждый разрешенный компонент самолета для установки или ремонта на данном самолете, имеет соответствующий идентификационный документ компонента самолета AC-ID, который содержит такие же цифровые данные компонента, как в обычном техническом паспорте (например, идентификационный код самолета, название изготовителя самолета, техническое название компонента, уникальный серийный номер компонента, название изготовителя компонента и дата изготовления компонента) вместе с дополнительными цифровыми данными, соответствующими идентификационному коду самолета, названию изготовителя самолета, дате сборки компонента на самолете, имени специалиста, ответственного за выполнение проверки соответствия, вместе с датой проверки соответствия и соответствующей (уникальной) цифровой подписи проверяющего. Кроме того, каждый идентификационный документ AC-ID компонента самолета защищен посредством нанесенной на него машиночитаемой защитной маркировки (предпочтительно защищенной от несанкционированного доступа). Предпочтительно, каждый раз при замене компонента или набора компонентов на самолете создаются соответствующие

защищенные документы AC-ID, а также создается соответствующая обновленная версия партии самолета с вышеупомянутыми соответствующими дополнительными цифровыми данными (относящимися к новым установочным операциям).

Таким образом, все (критически важные) установленные компоненты на конкретном самолете (в данном случае приведен самолет с идентификатором HB-SNO) принадлежат к соответствующей партии установленных компонентов (в данном случае всего □ компонентов). Защитная маркировка 310 (в данном случае в виде QR-кода) напечатана на каждом идентификационном документе компонента самолета, например, AC-ID: A_{125}, который связан с соответствующим компонентом самолета, в данном случае A_{125}, установленном на самолете HB-SNO. На фиг. 3, в частности, показан компонент A_{125} пакета самолета, представляющий собой лопатку турбины, адаптированную к типу реактора, установленную на самолете HB-SNO и маркированную уникальным заводским серийным номером (в данном случае 12781, обычно выгравированным изготовителем). Цифровые данные компонента D_{125} (или цифровые данные изделия), связанные с компонентом, A_{125} включают цифровые данные, соответствующие данным маркировки 330 данных, напечатанной на AC-ID:A125: идентификационный код 330a самолета (в данном случае HB-SNO), название 330b изготовителя самолета (в данном случае AeroABC), техническое название 330c компонента (в данном случае лопатка турбины - 1^{oe} кольцо), серийный номер 330d компонента (в данном случае 12781), название 330e изготовителя компонента (в данном случае PCX), дата изготовления компонента 330f (в данном случае 13 ноября 2017 г.), дата сборки компонента на реакторе 330g (в данном случае 24 февраля 2018 г.), имя специалиста, ответственного за выполнение проверки соответствия 330h (в данном случае проверяющий Мартин Вайт), вместе с датой проверки соответствия 330i (в данном случае 20 марта 2018 г.) и (уникальная) цифровая подпись проверяющего 330j (в данном случае 2w9s02u).

Цифровую подпись компонента x_{125} цифровых данных D_{125} AC-ID: A_{125} компонента A_{125} вычисляют посредством односторонней хеш-функции H в виде $x_{125} = H(D_{125})$. Таким же образом, все цифровые подписи компонента x_i цифровых данных D_i компонента A_i вычисляют посредством односторонней хеш-функции H в виде $x_i = H(D_i)$ (в данном случае i = 1,..., □). Пускай X соответствует всему набору цифровых подписей компонентов $X = (x_1, x_2, ..., x_\mu)$, и пускай X^i соответствует всему набору цифровых подписей компонентов, за исключением подписи x_i, то есть $X^i = (x_1, x_2,... * x_{i-1}, x_{i+1}, ..., X_\mu)$. Как уже раскрыто, агрегированную цифровую подпись B для партии μ компонентов самолета $A_1, ..., A_\mu$ вычисляют посредством одностороннего сумматора f в виде B = f(X). Агрегированную цифровую подпись затем сохраняют в доступной для поиска базе данных (предпочтительно, блокчейн), открытой для специалистов, ответственных за контроль или замену установленных компонентов.

Для заданного компонента A_i партии соответствующий ключ верификации k_i вычисляют посредством соответствующего частичного одностороннего сумматора в виде $k_i = f(X^i)$.. Для каждого компонента A_i, установленного на самолете HB-SNO, связанные цифровые данные компонента D_i и соответствующий ключ верификации k_i встроены в защитную маркировку, нанесенную на соответствующий идентификационный документ компонента самолета AC-ID: A_i. Например, в случае операции контроля компонента на самолете HB-SNO специалист может отправить запрос в доступную для поиска базу данных, содержащий серийный номер 12781 компонента, считываемый на AC-ID: A_{125} компонента A_{125}, подлежащего контролю, или его ключ верификации k_{125}, считываемый на защитной маркировке 310 на соответствующем документе AC-ID: A_{125} с помощью пригодного считывателя, и примет обратно соответствующее значение партии B. Однако, в предпочтительном варианте, обеспечивающем полную автономную проверку, считыватель специалиста подключен к компьютеру, имеющему память, сохраняющую все агрегированные цифровые подписи, относящиеся к самолетам, подлежащим контролю. В данном последнем варианте специалист затем может проверить, является ли компонент подлинным, путем считывания цифровых данных компонента D_{125} на защитной маркировке 310, проверки совпадения уникального серийного номера 330d (в данном случае 12781), извлеченного из D_{125}, с серийным номером, физически нанесенным на установленный компонент самолета A_{125}, вычисления соответствующей цифровой подписи компонента x_{125} (например, путем запуска запрограммированного приложения на ЦП компьютера, который вычисляет подпись $x_{125} = H(D_{125})$ из считанных цифровых данных D_{125}), вычисления потенциального значения партии B^c посредством функции одностороннего сумматора, запрограммированной на ЦП компьютера в виде $B^c = k_{125} \otimes x_{125}$ (оператор ⊗, соответствующий одностороннему сумматору f), и проверки совпадения потенциального значения партии B^c с одним из значений партии, сохраненных в памяти компьютера (то есть B, соответствующее самолету HB-SNO). В случае полного совпадения (то есть совпадения серийных номеров и B^c = B), компонент A_{125} считается подлинным и принадлежит к (обновленной) партии самолета разрешенных компонентов самолета HB-SNO, в случае несовпадения B^c с сохраненным значением партии B, или в случае несовпадения серийных номеров, компонент A_{125}, вероятно, является подделкой, или является подлинным компонентом, не разрешенным для самолета HB-SNO (например, A_{125} не принадлежит к правильной партии для данного самолета), и должен быть заменен.

Таким же образом, настоящее изобретение позволит обнаруживать мошенничество (или ошибки) в партиях защищенных AC-ID запасных деталей, хранящихся на складе, путем верификации аутентично-

сти защитных маркировок на хранимых деталях и проверки совпадения серийного номера компонента из защитной маркировки с номером, маркированным на соответствующем компоненте. В случае весьма критически важного компонента на компонент может быть дополнительно нанесена защищенная от несанкционированного доступа защитная маркировка на основе материала, в то время как цифровые данные, относящиеся к соответствующей контрольной уникальной физической характеристике UPC (например, снятые подходящим датчиком при нанесении защитной маркировки на основе материала) этой маркировки, предпочтительно являются частью цифровых данных компонента D в защитной маркировке этого компонента, и соответствующие контрольные данные уникальной физической подписи UPS вычисляются (например, путем взятия хеш-значения цифровых данных UPC, то есть UPS = H(UPC)) и могут также быть частью цифровых данных компонента. Этот дополнительный уровень безопасности повышает защиту, обеспечиваемую уникальным серийным номером, нанесенным на компонент его изготовителем. Предпочтительно, чтобы контрольные UPC и UPS хранились в блокчейне (чтобы обеспечить их неизменность) и были доступными для специалиста. Более того, эти контрольные значения могут также дополнительно храниться в памяти компьютера специалиста, чтобы обеспечить автономную аутентификацию защитной маркировки на основе материала на весьма критически важном компоненте.

Дальнейшая автономная операция аутентификации этой защитной маркировки на основе материала может включать измерение уникальной физической характеристики на компоненте посредством подходящего датчика, подключенного к компьютеру, и получение потенциальных цифровых данных уникальной физической характеристики UPC^c из измеренной характеристики (например, через специальное приложение, запрограммированное в ЦП его компьютера). Затем специалист (или ЦП его компьютера, если он соответствующим образом запрограммирован) сравнивает полученные UPC^c с копией контрольных UPC, сохраненных в памяти компьютера: в случае "обоснованного" совпадения $UPC^c \approx UPC$ (то есть в пределах некоторого заранее определенного критерия допустимых ошибок) защитная маркировка на основе материала и, следовательно, компонент считаются подлинными.

Как упомянуто выше, копия контрольных физических характеристических цифровых данные UPC, вместо того, чтобы храниться в памяти компьютера специалиста, является частью цифровых данных изделия D, включенных в защитную маркировку, нанесенную на компонент, и может быть получена путем непосредственного считывания на защитной маркировке (с помощью считывателя). Затем специалист может считать потенциальные UPC^c на защитной маркировке и проверить совпадение подписи UPS, сохраненной в памяти компьютера, с потенциальной подписью UPS^c, вычисленной из считанных потенциальных UPC^c путем вычисления $UPS^c = H(UPC^c)$: в случае совпадения $UPS^c = UPS$, подтверждается, что защитная маркировка на основе материала и, таким образом, компонент являются подлинными.

В варианте осуществления проверку аутентичности компонента специалистом можно альтернативно выполнять через процесс в режиме "онлайн" аналогично тому, как уже раскрыто в первом подробном варианте осуществления настоящего изобретения, и не будет повторяться в данном случае.

Согласно настоящему изобретению дополнительно возможно верифицировать соответствие цифрового изображения защищенного документа, такого как идентификационный документ компонента самолета AC-ID: A_{125}, например, относительно оригинального защищенного документа. В действительности, если специалист, ответственный за операции контроля (или ремонта), имеет только доступ к цифровому изображению защищенного документа, например, путем приема изображения AC-ID: A_{125} на его считывателе (который может быть, например, смартфоном, запрограммированным подходящим образом), он, тем не менее, может проверить соответствие данных компонента, напечатанных на принятом изображении документа, данным оригинального документа путем осуществления следующих операций: считывания цифровых данных компонента D_{125} и ключа верификации k_{125} на изображении защитной маркировки 310 на цифровом изображении документа AC-ID: A_{125}; получения контрольного значения B партии, соответствующего документу AC-ID: A_{125}; это контрольное значение может уже быть в памяти считывателя (или компьютера, подключенного к считывателю) или его можно получить посредством канала связи из базы данных, хранящей контрольные значения партии компонентов самолета, если считыватель оснащен блоком связи, путем отправки запроса, содержащего, например, (уникальный) серийный номер компонента или просто ключ k_{125}, считываемый на изображении защитной маркировки 310, и приема обратно соответствующего контрольного значения партии B; вычисления (с помощью запрограммированной односторонней функции H) цифровой подписи компонента x_{125} из считанных цифровых данных компонента D_{125}, с помощью $x_{125} = H(D_{125})$; вычисления потенциального значения партии (посредством запрограммированного одностороннего сумматора и его соответствующего оператора $\otimes$) B^c с $B^c = k_{125} \otimes x_{125}$; и верификации совпадения потенциального значения партии B^c с контрольным значением партии B.

Вышеупомянутые операции верификации соответствия также можно осуществлять на простой фотокопии оригинального документа $AC\text{-}ID_{125}$: действительно, даже если бы признак защиты от копирования был на защитной маркировке оригинального документа, который показал бы, что специалист имел только фотокопию, он, тем не менее, смог считать данные на защитной маркировке на фотокопии и выполнить вышеуказанные операции верификации соответствия данных, считанных на копии, относитель-

но оригинальных данных.

Другой иллюстративный вариант осуществления настоящего изобретения относится к самозащищенной сериализации фармацевтических продуктов, таких как упаковки с лекарственными препаратами, как показано на фиг. 4. Этот вариант осуществления относится к производственной партии упаковок с лекарственными препаратами данного типа лекарственного препарата, содержащей □ коробки (или изделия) A_1,A_2 ....A_μ. В этом иллюстративном примере типичной коробки A_1, показанной на фиг. 4, таблетки для пациентов упакованы в набор серийных блистерных упаковок 401 (показана только одна), содержащихся в коробке A_1. Каждая блистерная упаковка 401 маркирована уникальным серийным номером 435 (в данном случае 12345, нанесенным изготовителем), а на коробке A_1 напечатана обычная информация, такая как название лекарственного препарата 430a, логотип 430b, уникальный серийный номер коробки (идентификатор коробки) 430c, срок 430d годности. В этом примере дополнительные обычные данные, возможно, напечатаны на коробке (или, как вариант, на листке-вкладыше, вложенном в коробку A_1): рекомендуемая розничная цена 430e, страна 430f рынка сбыта и указание 430g ограничения продаж (например, продается только в аптеке). Коробка A_1 защищена машиночитаемой защитной маркировкой 410 в виде напечатанного двухмерного штрих-кода (или матрицы данных) и дополнительно защищена защитной маркировкой на основе материала в виде отдельного защищенного от несанкционированного доступа клейкого штампа 415 для защиты от копирования, включающего случайным образом диспергированные частицы, которая нанесена на коробку A_1. Известно, что (случайные и, следовательно, уникальные) положения частиц на штампе составляют уникальную физическую характеристику штампа 415, нанесенного на коробку A_1 и, таким образом, в данном случае также уникальную физическую характеристику самой коробки A_1. Обнаруженные положения диспергированных частиц на штампе 415 обычно используются для вычисления соответствующих контрольных цифровых данных уникальной физической характеристики UPC-A_1 коробки A_1. Обычно обнаружение диспергированных частиц и их положений осуществляют посредством обработки цифрового изображения штампа. В данном случае частицы могут быть обнаружены при освещении штампа простой белой вспышкой (например, белым светодиодом), как, например, вспышка смартфона. Предпочтительно на смартфон можно загрузить специальное приложение для обработки изображений, чтобы оно могло отображать штамп 415, обнаруживать положения диспергированных частиц и вычислять по этим положениям соответствующие цифровые данные уникальной физической характеристики UPC.

Согласно настоящему изобретению штрих-код 410 коробки A, ($i \in \{1,..., □\}$) партии содержит цифровые данные коробки D_i, соответствующие цифровому представлению вышеупомянутых обычных данных 430a-430g коробки A_i, соответствующих серийных номеров 435 блистерных упаковок 401, содержащихся в коробке A_i, и контрольных цифровых данных уникальной физической характеристики UPC-A_i коробки A_i. Для каждой коробки A_i партии связанную с коробкой цифровую подпись x_i его цифровых данных коробки D_i вычисляют посредством односторонней хеш-функции H в виде $x_i = H(D_i)$, i = 1,..., □. Пускай X обозначает набор всех цифровых подписей коробок партии, $X = (x_i,..., x_\mu)$ и X^i - набор всех цифровых подписей коробок, за исключением подписи x_i, то есть $X^i = (x_1, x_2, ... * x_{i-1}, x_{i+1}, ..., X_\mu)$. Контрольную агрегированную цифровую подпись B для всех коробок партии затем вычисляют посредством одностороннего сумматора f (и его соответствующего оператора ⊗) как B = f(X).

Например, односторонний сумматор f может соответствовать вышеупомянутому оператору ⊗, указывающему на (не только квази-коммутативное, но и коммутативное) модулярное умножение по заданному модулю m (то есть $a \otimes b = a*b \bmod m$) с $f(x) = x \bmod m$ и:

$$f(X) = f\big(f\big(f\big(\dots f(f(f(x_1), x_2), x_3), \dots, x_{\mu-2}\big), x_{\mu-1}\big), x_\mu\big) = f(x_1 \otimes x_2 \otimes x_3 \otimes \dots \otimes x_\mu) =$$

$$f(x_1) \otimes f(x_2) \otimes f(x_3) \otimes \dots \otimes f(x_\mu) = (x_1 \bmod m) * (x_2 \bmod m) * \dots * (x_\mu \bmod m) =$$

$$x_1 * x_2 * \dots * x_\mu \bmod m = x_1 \otimes x_2 \otimes \dots \otimes x_\mu,$$

или может соответствовать оператору ⊗, указывающему на квазикоммутативное возведение в степень по модулю m (то есть) $a \otimes b = a^b \bmod m$), с $f(x) = f(I; x) = I^x \bmod m$ (I представляет собой заданное целое число) и:

$$f(X) \equiv f(I; X) = f\big(f\big(f\big(\dots f(f(f(x_1), x_2), x_3), \dots, x_{\mu-2}\big), x_{\mu-1}\big), x_\mu\big) =$$

$$f(I; x_1 \otimes x_2 \otimes x_3 \otimes \dots \otimes x_\mu) = I \otimes \prod x_i = (I^{\prod x_i}) \bmod m, \text{ и } \prod x_i = x_1 * x_2 * \dots * x_\mu.$$

Полученная контрольная агрегированная цифровая подпись B затем либо опубликована в среде, открытой для пользователя, которому нужно проверить действительность защищенной упаковки с лекарственным препаратом A_i, либо сохранена в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, либо сохранена в блокчейне (или в базе данных, защищенной блокчейном), открытом для пользователя. Например, пользователь может отправить запрос, содержащий серийный номер 430c, считанный на защитной маркировке 410 на указанной коробке A_i, в доступную для поиска базу данных или в блокчейн и принять обратно соответствующее значение партии B. Ссылка для доступа к доступной для поиска базе данных агрегированных подписей (через Интернет, например) или блокчей-

ну могут быть включены в маркировку 440 данных коробки (показанную как QR-код на фиг. 4), напечатанную на коробке A_i.. Предпочтительно, контрольная агрегированная цифровая подпись B становится доступной для пользователя локально, так что пользователь может осуществлять операции проверки в автономном режиме (то есть не имея доступа к удаленным средствам хранения для получения B): например, пользователь имеет считыватель, такой как смартфон, выполненный с возможностью считывания и декодирования данных в защитной маркировке 410 на коробке A_i (посредством запрограммированного приложения, запущенного на ЦП смартфона) и память которого сохраняет контрольную агрегированную цифровую подпись B.

Для каждой коробки A_i. партии μ упаковок с лекарственными препаратами есть соответствующий ключ верификации k_i, вычисленный посредством частичного одностороннего сумматора f согласно формуле

$$k_i = f(X^i) = f\big(f\big(\dots f(f(f(x_1), x_2), x_3), \dots, x_{\mu-2}\big), x_{\mu-1}\big), x_\mu\big).$$

Цифровое значение коробки D_i и ее соответствующий ключ верификации коробки k_i (вместе составляющие информацию о верификации V_i коробки A_i) являются частью цифровых данных, включенных в защитную маркировку 410, нанесенную на коробку A_i.

Если символ ⊗ обозначает оператора, связанного с сумматором f, то для верификации аутентичности защищенной коробки A_1 согласно фиг. 4, принадлежащей к партии коробок, имеющих контрольную агрегированную цифровую подпись B, необходимо только считывание и декодирование цифровых данных коробки D_1 на защитной маркировке 410 на коробке A_1 (с помощью пригодного считывателя, например, с помощью вышеупомянутого смартфона, имеющего дополнительное запрограммированное приложение для вычисления подписи с помощью односторонней хеш-функции H и значения партии с оператором ⊗, соответствующим одностороннему сумматору f), вычисления соответствующей цифровой подписи коробки x_1 с помощью односторонней функции H как $x_1 = H(D_1)$, получения контрольной агрегированной цифровой подписи (значения партии) B (в данном примере контрольное значение партии B хранится в памяти считывателя) и проверки совпадения полученной контрольной агрегированной цифровой подписи B с потенциальной агрегированной цифровой подписью B^c, полученной из считанной информации о верификации (D_1, K_1) как $k_1 \otimes x_1$. Если $B^c \neq B$, то коробка A_1 является поддельной. Если $B^c = B$, то защитная маркировка 410 соответствует маркировке подлинной коробки. В этом случае можно выполнить несколько дополнительных проверок безопасности. Например, с помощью считывателя, оснащенного дисплеем (например, вышеупомянутого смартфона), можно извлечь из считанных цифровых данных коробки D_1 любую из информации 430a-430d, отобразить извлеченную информацию и визуально проверить ее совпадение с соответствующей информацией, напечатанной на коробке A_1. Если отображаемая информация не соответствует напечатанной, коробка является поддельной.

Возможна дополнительная проверка аутентичности коробки A_1 путем верификации подлинности защитной маркировки 415 на основе материала. Достаточно определить положения диспергированных частиц путем отображения штампа 415 (например, с помощью вышеупомянутого смартфона, выполненного с возможностью обработки изображений) и вычислить на основании этих положений соответствующие потенциальные цифровые данные уникальной физической характеристики UPC^c - A_1, а затем проверить действительную схожесть этих UPC^c - A_1 (в пределах заданной погрешности) с контрольными цифровыми данными уникальной физической характеристики UPC^c - A_1, извлеченными из цифровых данных коробки D_1: если они схожи, то штамп 415, и, таким образом, коробка A_1, является подлинным, если они не схожи, то штамп 415, и, таким образом, коробка A_1 (штамп является защищенным от несанкционированного доступа), является поддельным.

Тем не менее, в случае верифицированного совпадения агрегированных цифровых подписей (то есть $B^c = B$), и даже если информация 430a-430d была верифицирована и/или защитная маркировка 415 на основе материала является подлинной, дополнительно можно проверить, являются ли блистерные упаковки 401, содержащиеся в коробке A_1, правильными: достаточно проверить совпадение уникальных серийных номеров 435, маркированных на блистерных упаковках, с номерами, указанными цифровыми данными коробки D_1, считанными из защитной маркировки 410. В случае несовпадения этих данных, это является доказательством подделки: блистерные упаковки подлинной коробки A_1 были заменены другими (возможно, поддельными, или другой марки, или соответствующими другому лекарственному препарату). Более того, все еще в случае подлинной коробки A_1 (то есть с $B^c = B$), даже если блистерные упаковки 401 являются правильными, в случае если любая дополнительная информация, извлеченная из цифровых данных коробки D_1: рекомендованная розничная цена 430e, страна 430f рынка сбыта и указание 430g ограничения продажи, не соответствует существующим условиям продажи (например, если упаковка с лекарственным препаратом A_1 продается в стране, отличной от указанной данными 430f), можно обнаружить соответствующее мошенничество. Это также является серьезным предупреждением о том, что сама партия или по меньшей мере ее часть были перенаправлены.

Таким образом, как операции полного отслеживания и контроля, так и проверки аутентичности защищенных упаковок с лекарственными препаратами возможны благодаря защищенной от подделки связи, обеспечиваемой согласно настоящему изобретению посредством агрегированной цифровой подписи

между данными коробки, данными содержащихся блистерных упаковок, уникальными характеризующими физическими свойствами коробки и блистерными упаковками, а также принадлежностью коробки к данной партии.

Согласно вышеприведенному подробному описанию настоящее изобретение явно совместимо с операциями автономной и локальной проверки для верификации аутентичности защищенного изделия или соответствия данных на изображении (или копии) защищенного изделия относительно данных, связанных с оригинальным защищенным изделием. Однако настоящее изобретение также совместимо с процессом верификации в режиме "онлайн", например, путем приема (через канал связи) контрольного значения партии из внешнего источника (например, сервера или блокчейна) или выполнения некоторых или всех этапов вычисления, включающих одностороннюю функцию или односторонний сумматор через внешние вычислительные средства (например, работающие на сервере), или даже выполнения верификации совпадения потенциальной агрегированной цифровой подписи с контрольной агрегированной цифровой подписью (и просто получение результата).

Вышеуказанный предмет изобретения следует считать иллюстративным, а не ограничивающим, и он служит для лучшего понимания настоящего изобретения, определяемого независимыми пунктами формулы изобретения.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ защиты заданного оригинального изделия из партии множества оригинальных изделий от подделки или фальсификации, при этом каждое оригинальное изделие партии имеет собственные связанные с ним данные изделия и соответствующие цифровые данные изделия, отличающийся тем, что способ включает этапы:

для каждого оригинального изделия партии вычисления посредством односторонней функции связанной с изделием цифровой подписи его соответствующих цифровых данных изделия;

вычисления контрольной агрегированной цифровой подписи, соответствующей партии оригинальных изделий, из всех цифровых подписей оригинальных изделий партии посредством одностороннего сумматора указанных цифровых подписей изделий, и предоставления в распоряжение пользователя контрольной агрегированной цифровой подписи;

определения ключа верификации изделия, соответствующего цифровой подписи указанного заданного оригинального изделия, посредством частичного одностороннего сумматора всех других цифровых подписей изделий, используемых для вычисления контрольной агрегированной цифровой подписи, в результате чего потенциальная цифровая подпись изделия соответствует подписи оригинального изделия партии, в случае вычисления контрольной агрегированной цифровой подписи из указанной потенциальной цифровой подписи изделия и соответствующего ключа верификации изделия посредством односторонней функции; и

нанесения на заданное оригинальное изделие соответствующей машиночитаемой защитной маркировки, включающей представление связанных с изделием цифровых данных и его соответствующего ключа верификации изделия, тем самым получая маркированное оригинальное изделие, данные изделия которого защищены от подделки или фальсификации.

2. Способ по п.1, отличающийся тем, что контрольная агрегированная цифровая подпись, связанная с партией оригинальных изделий, либо опубликована в среде, открытой для пользователя, либо сохранена в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, либо сохранена в блокчейне, либо в базе данных, защищенной блокчейном, открытой для пользователя.

3. Способ по п.2, отличающийся тем, что маркированное оригинальное изделие дополнительно содержит данные по доступу к агрегированным подписям, маркированные на нем и содержащие информацию, достаточную для получения доступа к контрольной агрегированной цифровой подписи, соответствующей партии оригинальных изделий, при этом указанная информация представляет собой ссылку в интерфейс сбора агрегированных подписей, соответственно, одного из следующего:

среда, в которой опубликована контрольная агрегированная цифровая подпись, при этом среда является открытой для пользователя посредством указанного интерфейса сбора агрегированных подписей, выполненного с возможностью приема от пользователя запроса на агрегированную подпись, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной агрегированной цифровой подписи связанной партии;

доступная для поиска база данных агрегированных подписей, в которой сохранена контрольная агрегированная цифровая подпись, при этом база данных агрегированных подписей является открытой для пользователя посредством указанного интерфейса сбора агрегированных подписей, выполненного с возможностью приема от пользователя запроса на агрегированную подпись, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной агрегированной цифровой подписи связанной партии;

блокчейн, соответственно, база данных, защищенная блокчейном, в котором сохранена агрегированная цифровая подпись с временной меткой, при этом блокчейн, соответственно, база данных, защищенная блокчейном, является открытым для пользователя посредством указанного интерфейса сбора агрегированных подписей, выполненного с возможностью приема от пользователя запроса на агрегированную подпись, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной агрегированной цифровой подписи связанной партии.

4. Способ по любому из пп.1-3, отличающийся тем, что виртуальное изделие включено в партию оригинальных изделий, при этом указанное виртуальное изделие имеет связанные с виртуальным изделием данные и его соответствующие цифровые данные виртуального изделия, а также связанную с виртуальным изделием цифровую подпись, получаемую посредством односторонней функции, при этом указанное виртуальное изделие не создается, а только используется для генерирования связанной с виртуальным изделием цифровой подписи из соответствующих цифровых данных виртуального изделия; и контрольная агрегированная цифровая подпись, связанная с указанной партией оригинальных изделий, вычислена из всех цифровых подписей оригинальных изделий партии, включающих цифровую подпись виртуального изделия, посредством одностороннего сумматора.

5. Способ по любому из пп.1-4, отличающийся тем, что односторонняя функция представляет собой хеш-функцию, а цифровая подпись оригинального изделия представляет собой последовательность заданного множества битов с меньшими значениями разряда, выбранных из битов хеш-значения соответствующих цифровых данных изделия.

6. Способ по любому из пп.1-5, отличающийся тем, что дополнительные цифровые данные изделия, соответствующие данным изделия, связанным с маркированным оригинальным изделием, сохранены в доступной для поиска информационной базе данных, открытой для пользователя, посредством интерфейса информационной базы данных, выполненного с возможностью приема от пользователя запроса на информацию, содержащего данные изделия или соответствующие данные цифровой подписи, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно соответствующих дополнительных цифровых данных изделия.

7. Способ по любому из пп.1-6, отличающийся тем, что маркированное оригинальное изделие дополнительно содержит соответствующую маркировку данных изделия, нанесенную на него, при этом указанная маркировка данных изделия включает соответствующие данные изделия, связанные с указанным маркированным оригинальным изделием.

8. Способ по любому из пп.1-7, отличающийся тем, что цифровые данные маркированного оригинального изделия включают контрольные физические характеристические цифровые данные UPC соответствующей уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека.

9. Способ по п.8, отличающийся тем, что уникальная физическая характеристика маркированного оригинального изделия представляет собой характеристику защитной маркировки на основе материала, нанесенной на оригинальное изделие.

10. Способ верификации аутентичности изделия, защищенного согласно способу по любому из пп.1-9, или соответствия копии такого защищенного изделия относительно оригинального изделия, отличающийся тем, что способ включает этапы, при рассматривании тестового объекта, представляющего собой указанное изделие или указанную копию изделия:

получения цифрового изображения защитной маркировки на тестовом объекте посредством устройства для формирования изображения, имеющего блок формирования изображения, ЦП с памятью и блок обработки изображения;

считывания представления цифровых данных изделия и связанного с изделием ключа верификации на полученном цифровом изображении защитной маркировки на тестовом объекте и извлечения, соответственно, соответствующих цифровых данных изделия и ключа верификации изделия из указанного считанного представления;

сохранения в памяти контрольной агрегированной цифровой подписи соответствующей партии изделий и программирования в ЦП односторонней функции и одностороннего сумматора;

верификации действительного соответствия извлеченных цифровых данных изделия и связанного с изделием ключа верификации сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов:

вычисления цифровой подписи извлеченных цифровых данных изделия с помощью односторонней функции;

вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных изделия и извлеченного ключа верификации изделия с помощью одностороннего сумматора; и

проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего, в случае совпадения указанных агрегированных цифровых подписей, данные изделия на тестовом объекте являются данными подлинного

оригинального изделия.

11. Способ по п.10, отличающийся тем, что изделие защищено путем сохранения контрольной агрегированной цифровой подписи, связанной с партией оригинальных изделий, в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, согласно способу по п.2, и устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, при этом способ включает этапы:

отправки блоком связи посредством канала связи запроса в указанную базу данных агрегированных подписей и приема обратно контрольной агрегированной цифровой подписи, связанной с партией оригинальных изделий; и

сохранения принятой агрегированной цифровой подписи в памяти устройства для формирования изображения, что предшествует этапам, указанным в п.10.

12. Способ по п.10, отличающийся тем, что изделие защищено согласно способу по п.3, и устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, при этом способ включает этапы:

считывания данных по доступу к агрегированным подписям, маркированных на тестовом объекте, с помощью устройства для формирования изображения;

отправки блоком связи посредством канала связи запроса на агрегированную подпись в указанный интерфейс сбора агрегированных подписей, содержащего данные изделия или цифровую подпись указанных данных изделия, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующей контрольной агрегированной цифровой подписи связанной партии; и

сохранения принятой агрегированной цифровой подписи в памяти устройства для формирования изображения, что предшествует этапам, указанным в п.10.

13. Способ по любому из пп.10-12, отличающийся тем, что изделие защищено согласно способу по п.6, и устройство для формирования изображения дополнительно оснащено средствами связи, выполненными с возможностью отправки в интерфейс информационной базы данных запроса на информацию, содержащего данные изделия или соответствующие данные цифровой подписи, получаемые из защитной маркировки на тестовом изделии, и приема обратно соответствующих дополнительных цифровых данных изделия.

14. Способ по любому из пп.10-13, отличающийся тем, что изделие защищено согласно способу по п.7, при этом способ включает дополнительные этапы:

считывания данных изделия, маркированных на маркировке данных изделия на тестовом объекте, с помощью устройства для формирования изображения; и

проверки соответствия данных изделия, считанных из маркировки данных изделия, цифровым данным изделия, извлеченным из защитной маркировки на тестовом объекте.

15. Способ по любому из пп.10-14, отличающийся тем, что изделие защищено согласно способу по любому из пп.8 и 9, и устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека, и ЦП запрограммирован для извлечения соответствующих цифровых данных уникальной физической характеристики из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные физические характеристические цифровые данные UPC, соответствующие указанной уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека, при этом способ включает дополнительные этапы, при рассматривании субъекта, представляющего собой указанное изделие или указанный связанный объект или человека:

обнаружения с помощью датчика уникальной физической характеристики субъекта и извлечения соответствующих потенциальных цифровых данных уникальной физической характеристики UPC^c;

сравнения полученных потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC; и

в случае схожести потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC при условии заданного критерия допустимого отклонения субъект считается подлинным.

16. Маркированное изделие, принадлежащее к партии множества оригинальных изделий и защищенное от подделки или фальсификации согласно способу по любому из пп.1-9, при этом каждое оригинальное изделие партии имеет собственные связанные с ним данные изделия и соответствующие цифровые данные изделия, указанная партия имеет соответствующую контрольную агрегированную цифровую подпись, при этом изделие содержит: машиночитаемую защитную маркировку, нанесенную на него и включающую представление связанных с изделием цифровых данных и соответствующего ключа верификации изделия.

17. Маркированное изделие по п.16, отличающееся тем, что цифровые данные маркированного изделия включают контрольные физические характеристические цифровые данные UPC соответствующей уникальной физической характеристики маркированного изделия или связанного объекта или человека.

18. Маркированное изделие по п.17, отличающееся тем, что уникальная физическая характеристика

маркированного изделия представляет собой характеристику защитной маркировки на основе материала, нанесенной на маркированное изделие.

19. Система верификации аутентичности маркированного оригинального изделия, защищенного согласно способу по любому из пп.1-9, или соответствия копии такого изделия относительно оригинального изделия, при этом система содержит устройство для формирования изображения, имеющее блок формирования изображения, ЦП с памятью и блок обработки изображения, при этом память сохраняет контрольную агрегированную цифровую подпись соответствующей партии изделий и одностороннюю функцию и односторонний сумматор, запрограммированные в ЦП, при этом система выполнена с возможностью:

получения цифрового изображения защитной маркировки на тестовом объекте, представляющем собой указанное изделие или указанную копию изделия;

считывания представления цифровых данных изделия и связанного с изделием ключа верификации на полученном цифровом изображении защитной маркировки на тестовом объекте и извлечения, соответственно, соответствующих цифровых данных изделия и ключа верификации изделия из указанного считанного представления;

верификации действительного соответствия извлеченных цифровых данных изделия и связанного ключа верификации сохраненной контрольной агрегированной цифровой подписи путем осуществления на ЦП дополнительных запрограммированных этапов:

вычисления цифровой подписи извлеченных цифровых данных изделия с помощью односторонней функции;

вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных изделия и извлеченного ключа верификации с помощью одностороннего сумматора; и

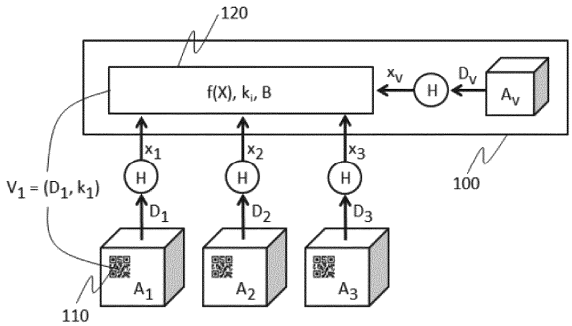
проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего в случае совпадения указанных агрегированных цифровых подписей система выполнена с возможностью доставки указания того, что данные изделия на тестовом объекте являются данными подлинного оригинального изделия.

20. Система по п.19 для верификации изделия, защищенного согласно способу по любому из п.8 и 9, отличающаяся тем, что устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека, и ЦП запрограммирован для извлечения соответствующих цифровых данных уникальной физической характеристики из сигнала обнаружения, принятого от датчика, при этом устройство для формирования изображения сохраняет в памяти контрольные физические характеристические цифровые данные UPC, соответствующие указанной уникальной физической характеристике маркированного оригинального изделия или связанного объекта или человека, при этом система дополнительно выполнена с возможностью:

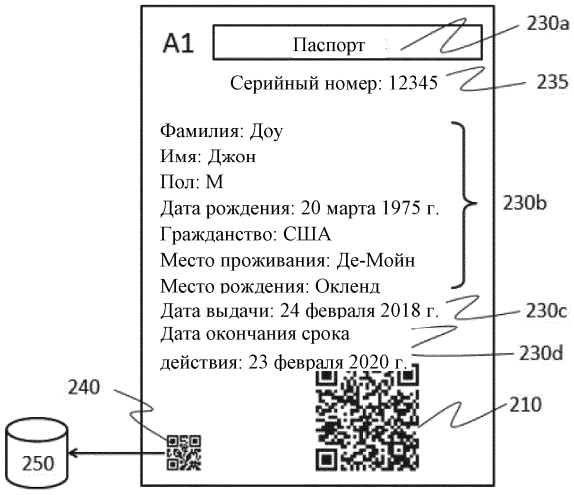
обнаружения с помощью датчика уникальной физической характеристики субъекта, представляющего собой указанное изделие или указанный связанный объект или человека, и извлечения соответствующих потенциальных цифровых данных уникальной физической характеристики UPC^c;

сравнения полученных потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC; и

в случае схожести потенциальных цифровых данных уникальной физической характеристики UPC^c с сохраненными контрольными физическими характеристическими цифровыми данными UPC, при условии заданного критерия допустимого отклонения, доставки указания того, что субъект считается подлинным.

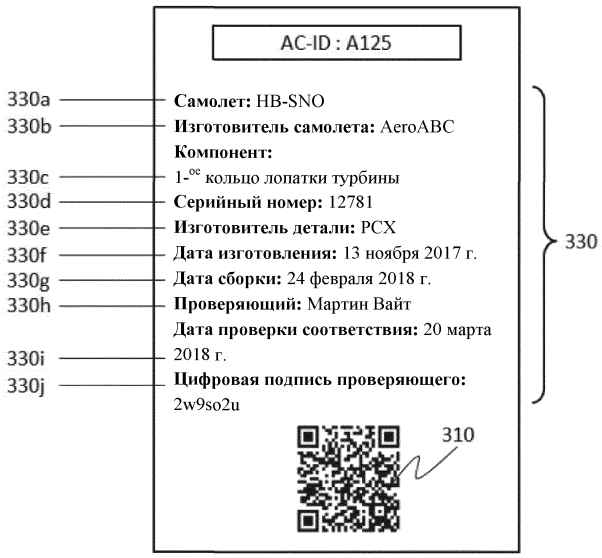


Фиг. 1

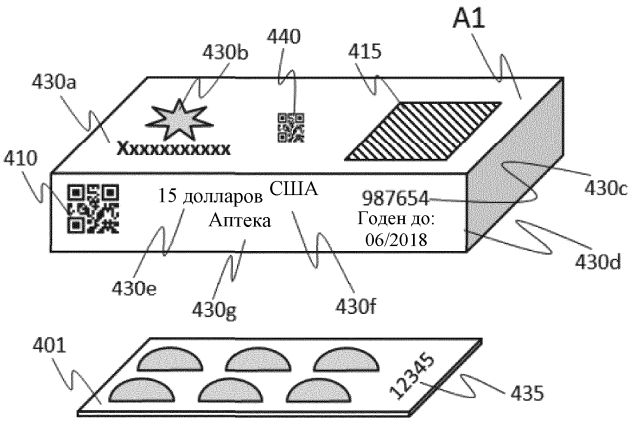


Фиг. 2A

Фиг. 2B



Фиг. 3


A1
440
430b
415
430a
Xxxxxxxxxx
410
15 долларов
США
987654
430c
Аптека
Годен до:
06/2018
430d
430e
430g
430f
401
12345
435

Фиг. 4