(19) Евразийское патентное ведомство

(11) 040918 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.08.17

(21) Номер заявки
202190227

(22) Дата подачи заявки
2019.06.03

(51) Int. Cl. ***B42D 25/24*** (2014.01)
B42D 25/28 (2014.01)
B42D 25/21 (2014.01)
B42D 25/305 (2014.01)
B42D 25/405 (2014.01)
B42D 25/48 (2014.01)
B42D 13/00 (2006.01)
G09F 3/00 (2006.01)
H04L 9/00 (2006.01)
G06K 7/00 (2006.01)
G07D 7/00 (2016.01)

(54) ЗАЩИТА ИЗДЕЛИЯ ОТ ПОДДЕЛКИ

(31) **18182697.5**
(32) **2018.07.10**
(33) **EP**
(43) **2021.05.31**
(86) **PCT/EP2019/064359**
(87) **WO 2020/011447 2020.01.16**

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

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

(74) Представитель:
Абильманова К.С. (KZ)

(56) EP-A1-3340213
EP-A1-3340212
EP-A2-2131310
US-A1-2002184504
US-A1-2018189312
US-A-4309569

(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.

040918 B1

040918 B1

Область техники, к которой относится изобретение

Настоящее 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), т.е. 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 защищенного объекта.

Краткое описание изобретения

Согласно одному аспекту настоящее изобретение относится к способу защиты заданного оригинального изделия, принадлежащего к партии множества оригинальных изделий, от подделки или фальсификации, при этом каждое оригинальное изделие 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;

формирования дерева на основании множества вычисленных цифровых подписей изделий для оригинальных изделий партии, содержащего узлы, расположенные согласно заданной упорядоченности узлов в дереве, при этом указанное дерево содержит уровни узлов, начиная от листовых узлов, соответствующих множеству цифровых подписей изделий, соответственно, связанных с множеством оригинальных изделий в партии, до корневого узла дерева, каждый узел, отличный от листового, дерева соответствует цифровой подписи посредством односторонней функции конкатенации соответственных цифровых подписей его дочерних узлов согласно упорядоченности конкатенации дерева, корневой узел соответствует контрольной корневой цифровой подписи, т.е. цифровой подписи посредством односторонней функции конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

связывания с заданным оригинальным изделием соответствующего ключа верификации, представляющего собой последовательность соответственных цифровых подписей, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел, соответствующий цифровой подписи заданного оригинального изделия, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне;

предоставления в распоряжение пользователя контрольной корневой цифровой подписи дерева; и

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

Контрольная корневая цифровая подпись корневого узла дерева может быть либо опубликована в среде, открытой для пользователя, либо сохранена в доступной для поиска корневой базе данных, открытой для пользователя, либо сохранена в блокчейне, либо сохранена в базе данных, защищенной блокчейном, открытой для пользователя.

Таким образом, согласно настоящему изобретению переплетение цифровых подписей всех изделий партии, благодаря структуре дерева и использованию надежных односторонних функций для вычисления значений узлов, вместе с корневой цифровой подписью дерева, сделанной неизменной, и включение цифровых данных изделия и связанного с ним ключа верификации в защитную маркировку, нанесенную на соответствующее изделие, позволяют отслеживать и контролировать маркированные изделия с очень высоким уровнем надежности, при этом предотвращая фальсификацию данных и подделку маркированных изделий.

Маркированное оригинальное изделие может дополнительно содержать данные по доступу к корневому узлу, маркированные на нем и содержащие информацию, достаточную для обеспечения доступа пользователю к контрольной корневой цифровой подписи корневого узла дерева, соответствующего партии оригинальных изделий, при этом указанная информация является ссылкой в интерфейс доступа, выполненный с возможностью приема от пользователя корневого запроса, содержащего цифровые данные изделия или цифровую подпись цифровых данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной корневой цифровой подписи соответствующего дерева, при этом интерфейс доступа обеспечивает доступ, соответственно, к одному из следующего:

среда, в которой опубликована контрольная корневая цифровая подпись;

доступная для поиска корневая база данных, в которой сохранена контрольная корневая цифровая подпись; и

блокчейн или, соответственно, база данных, защищенная блокчейном, в котором сохранена контрольная корневая цифровая подпись с временной меткой.

Согласно настоящему изобретению также возможно, что

виртуальное изделие считается принадлежащим к партии 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 цифровых данных виртуального изделия, указанное виртуальное изделие не создается, а только используется для генерирования связанной с виртуальным

изделием цифровой подписи; и

контрольная корневая цифровая подпись, связанная с указанной партией оригинальных изделий, вычислена из дерева, имеющего все цифровые подписи оригинальных изделий партии, включающие цифровую подпись виртуального изделия, в виде листовых узлов.

С целью получения более коротких подписей, 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 цифровые данные изделия или цифровую подпись цифровых данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно соответствующих дополнительных цифровых данных изделия. Дополнительные цифровые данные изделия, соответствующие цифровым данным изделия, связанным с маркированным оригинальным изделием, могут дополнительно быть конкатенированы с указанными цифровыми данными изделия, в результате чего дополнительные цифровые данные изделия также защищены от подделки или фальсификации.

Более того, 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.

Вышеупомянутые цифровые данные маркированного оригинального изделия могут включать соответствующие контрольные характеристические цифровые данные 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 или на связанный объект.

В вышеуказанном способе последовательность цифровых подписей ключа верификации, включенного в защитную маркировку изделия, может быть расположена согласно упорядоченности последовательности узлов, которая отличается от упорядоченности соответствующих узлов, определенных упорядоченностью конкатенации дерева, и защитная маркировка изделия может дополнительно включать код упорядоченности, связанный с указанной упорядоченностью последовательности.

Согласно настоящему изобретению в случае распределения цифровых данных соответственных оригинальных изделий партии между заданными полями, общими для всех изделий партии, цифровые данные, относящиеся к этим полям, могут не быть включены в цифровые данные изделия, но могут быть сгруппированы в отдельный блок данных полей, связанный с партией, и при этом

i) цифровую подпись оригинального изделия вычисляют с помощью односторонней функции конкатенации соответствующих цифровых данных изделия и цифровых данных блока данных полей; и

ii) контрольная корневая цифровая подпись поступает в распоряжение пользователя вместе со связанным блоком данных полей.

Другой аспект настоящего изобретения относится к способу верификации аутентичности изделия или соответствия копии такого изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно вышеуказанному способу защиты, 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, блок обработки с памятью и блок обработки изображения;

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

сохранения в памяти контрольной корневой цифровой подписи корневого узла дерева партии оригинальных изделий и программирования в блоке обработки односторонней функции для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и связанного тестового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления этапов:

вычисления с помощью односторонней функции тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому

листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов, извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей, данные изделия на тестовом объекте являются данными подлинного изделия.

Если маркированное оригинальное изделие защищено, при этом имея вышеупомянутый отдельный блок данных полей, память блока обработки может дополнительно сохранять указанный связанный блок данных полей, и этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, может включать вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

Если изделие было защищено путем сохранения контрольной корневой цифровой подписи в доступной для поиска корневой базе данных, открытой для пользователя, устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, вышеуказанный способ верификации может включать предварительные этапы

отправки блоком связи посредством канала связи запроса в указанную корневую базу данных и приема обратно контрольной корневой цифровой подписи и

сохранения принятой корневой цифровой подписи в памяти устройства для формирования изображения.

Если защищенное изделие содержит данные по доступу к корневому узлу, как раскрыто выше, и устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема данных посредством канала связи, вышеуказанный способ верификации может включать предварительные этапы

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

отправки блоком связи посредством канала связи корневого запроса в указанный интерфейс доступа, содержащего цифровые данные изделия или цифровую подпись указанных цифровых данных изделия, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующей контрольной корневой цифровой подписи связанной партии; и

сохранения принятой контрольной корневой цифровой подписи в памяти устройства для формирования изображения.

Защищенное изделие может содержать дополнительные цифровые данные изделия, как раскрыто 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 цифровые данные изделия или соответствующие данные цифровой подписи изделия, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующих дополнительных цифровых данных изделия.

Если защищенное изделие содержит маркировку данных изделия, как раскрыто выше, способ может включать 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.

Более того, если защищенное изделие включает контрольные характеристические цифровые данные, как раскрыто выше, и устройство для формирования изображения дополнительно оснащено датчи-

ком, выполненным с возможностью обнаружения уникальной физической характеристики соответственно маркированного оригинального изделия или связанного объекта или человека, и блок обработки запрограммирован для извлечения соответствующих характеристических цифровых данных из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике соответственно маркированного оригинального изделия или связанного объекта или человека, вышеуказанный способ может включать 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 характеристических цифровых данных CDD^c;

сравнения полученных потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD; и

в случае схожести потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD, с заданным критерием допустимого отклонения, субъект считается соответствующим, соответственно, подлинному изделию или объекту или человеку, действительно связанному с подлинным изделием.

Дополнительный аспект настоящего изобретения относится к способу верификации соответствия цифрового изображения изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно вышеупомянутому способу защиты, при этом способ включает этапы

получения цифрового изображения изделия, демонстрирующего защитную маркировку на изделии, посредством устройства для формирования изображения, имеющего блок формирования изображения, блок обработки с памятью и блок обработки изображения;

считывания представления цифровых данных изделия и связанного ключа верификации на полученном цифровом изображении защитной маркировки и извлечения, соответственно, соответствующих тестовых цифровых данных изделия и связанного тестового ключа верификации из указанного считанного представления;

сохранения в памяти контрольной корневой цифровой подписи корневого узла дерева партии оригинальных изделий и программирования в блоке обработки односторонней функции для вычисления цифровой подписи цифровых данных и

конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и тестового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления этапов

вычисления с помощью односторонней функции тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов, извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей, цифровое изображение изделия является изображением подлинного маркированного оригинального изделия.

Если партия защищенного маркированного оригинального изделия имеет связанный блок данных полей, как раскрыто выше, память блока обработки дополнительно сохраняет связанный блок данных полей, этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, может включать вычисление

с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

Если оригинальное изделие было защищено путем сохранения контрольной корневой цифровой подписи в доступной для поиска корневой базе данных, открытой, как упомянуто выше, и устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема обратно данных посредством канала связи, способ может включать предварительные этапы

отправки блоком связи посредством канала связи запроса в указанную корневую базу данных и приема обратно контрольной корневой цифровой подписи; и

сохранения принятой корневой цифровой подписи в памяти устройства для формирования изображения.

Если оригинальное изделие содержит данные по доступу к корневому узлу, как упомянуто выше, и устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема данных посредством канала связи, способ может включать предварительные этапы

считывания данных по доступу к корневому узлу, маркированных на цифровом изображении изделия, с помощью устройства для формирования изображения;

отправки блоком связи посредством канала связи корневого запроса в интерфейс доступа, содержащего извлеченные тестовые цифровые данные изделия или вычисленную тестовую цифровую подпись, и приема обратно контрольной корневой цифровой подписи корневого узла дерева партии оригинальных изделий; и

сохранения принятой контрольной корневой цифровой подписи в памяти устройства для формирования изображения.

Если маркированное оригинальное изделие имеет связанные с изделием дополнительные цифровые данные, сохраненные в доступной для поиска информационной базе данных, как упомянуто выше, устройство для формирования изображения может дополнительно быть оснащено средствами связи, выполненными с возможностью отправки в интерфейс информационной базы данных запроса на информацию, содержащего тестовые цифровые данные изделия или тестовые данные цифровой подписи изделия, и приема обратно соответствующих дополнительных цифровых данных изделия.

Если защищенное оригинальное изделие включает контрольные характеристические цифровые данные, как упомянуто выше, и устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики соответственно объекта или человека, связанного с маркированным оригинальным изделием, и блок обработки запрограммирован для извлечения соответствующих характеристических цифровых данных из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике соответственно связанного объекта или человека, способ может включать дополнительные этапы при рассматривании субъекта, представляющего собой указанный связанный объект или человека:

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

сравнения полученных потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD; и

в случае схожести потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD, с заданным критерием допустимого отклонения, субъект считается соответствующим, соответственно, объекту или человеку, действительно связанному с подлинным маркированным оригинальным изделием.

Другой аспект настоящего изобретения относится к изделию, принадлежащему к партии множества оригинальных изделий и защищенному от подделки или фальсификации согласно вышеупомянутому способу защиты, при этом каждое оригинальное изделие партии имеет свои собственные цифровые данные изделия и соответствующий ключ верификации, указанная партия имеет соответствующую контрольную корневую цифровую подпись, при этом изделие содержит

машиночитаемую защитную маркировку, нанесенную на изделие и включающую представление его цифровых данных изделия и его ключа верификации.

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

Другой аспект настоящего изобретения относится к системе верификации аутентичности изделия или соответствия копии такого изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных двойной материальной и цифровой защитой от подделки или фальсификации согласно вышеупомянутому способу защиты, при этом система содержит

устройство для формирования изображения, имеющее блок формирования изображения, блок обработки с памятью и блок обработки изображения, при этом память сохраняет контрольную корневую цифровую подпись дерева, соответствующего партии оригинальных изделий, и одностороннюю функцию для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, запрограммированной в блоке обработки, при этом указанная система выполнена с возможностью

получения с помощью устройства для формирования изображения цифрового изображения защитной маркировки на тестовом объекте, представляющем собой указанное изделие или указанную копию изделия;

считывания с помощью устройства для формирования изображения представления цифровых данных изделия и связанного ключа верификации на полученном цифровом изображении защитной маркировки на тестовом объекте и извлечения, соответственно, соответствующих тестовых цифровых данных изделия и тестового ключа верификации из указанного считанного представления;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и связанного ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления на блоке обработки дополнительных запрограммированных этапов

вычисления с помощью односторонней функции тестовой цифровой подписи из вычисленной тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов, извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей, система выполнена с возможностью доставки указания того, что данные изделия на тестовом объекте являются данными подлинного изделия.

Если маркированное оригинальное изделие имеет связанный блок данных полей, как упомянуто выше, память блока обработки дополнительно сохраняет связанный блок данных полей, этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, затем включает вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

Другой аспект настоящего изобретения относится к системе верификации соответствия цифрового изображения изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно вышеупомянутому способу защиты, при этом система содержит устройство для формирования изображения, имеющее блок формирования изображения, блок обработки с памятью и блок обработки изображения, при этом память сохраняет контрольную корневую цифровую подпись дерева, соответствующего партии оригинальных изделий, и одностороннюю функцию для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, запрограммированной в блоке обработки, при этом указанная система выполнена с возможностью

получения цифрового изображения изделия, демонстрирующего защитную маркировку на изделии, посредством устройства для формирования изображения;

считывания с помощью устройства для формирования изображения представления цифровых данных изделия и связанного ключа верификации на полученном цифровом изображении защитной маркировки и извлечения, соответственно, соответствующих тестовых цифровых данных изделия и связанного тестового ключа верификации из указанного считанного представления;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и тестового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления на блоке обработки дополнительных запрограммированных этапов

вычисления с помощью односторонней функции тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов, извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей, система выполнена с возможностью доставки указания того, что цифровое изображение изделия является изображением подлинного маркированного оригинального изделия.

Если маркированное оригинальное изделие имеет связанный блок данных полей, как упомянуто выше, память блока обработки дополнительно сохраняет связанный блок данных полей, этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, может включать вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

Далее настоящее изобретение будет описано более полно со ссылкой на прилагаемые чертежи, на которых одинаковые цифры представляют одинаковые элементы на разных фигурах и 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 - защищенный биометрический паспорт в качестве примера биометрического документа, удостоверяющего личность, защищенного согласно настоящему изобретению,

на фиг. 2B - контроль человека, имеющего защищенный биометрический паспорт согласно фиг. 2A, уполномоченным сотрудником,

на фиг. 3 - партия компонентов самолета, защищенных согласно настоящему изобретению,

на фиг. 4 - 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 и связанное с ними дерево, при этом для упрощения показаны только восемь изделий: A_1, ..., A_8, которые могут представлять собой что угодно, способное нести или содержать физическую машиночитаемую защитную маркировку 110 (в данном случае проиллюстрированную двухмерным штрих-кодом, но может быть одномерным штрих-кодом или маркировкой RFID и т.д.), 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. Любое из изделий, показанных на фиг. 1, может представлять собой "виртуальное изделие" A_v, которое является необязательным средством программного обеспечения, которое может быть включено для обеспечения кодирования выбранных данных. Это объясняется далее. Например, одно из восьми изделий, например изделие A_8, может фактически представлять собой виртуальное изделие A_v, которое считается принадлежащим к партии из восьми изделий, и обработано как любое из других семи реальных изделий A_1, A_2, A_3, ..., поскольку оно может быть обработано, по существу, таким же путем (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_7, A_vA_1, A_2, A_3, ..., A_v партии (где $A_8 \equiv A_v$) соответственные цифровые данные изделия D_1, D_2, ..., D_7, D_v (где $D_8 \equiv D_v$) связаны или извлечены (или в случае виртуального изделия A_v созданы) с использованием 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_iD_i.

Для виртуального изделия A_vA_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, информацию 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 партии его соответственные цифровые данные изделия D_1, D_2, ..., D_7, D_vD_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, т.е. 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, т.е. 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_8 представляют собой хеш-значения, т.е. связанные с изделиями цифровые подписи соответственных наборов данных изделий, а именно $x_j = H(D_j)$, для j=1, ..., 8 (в случае $A_8 \equiv A_v$, то $D_8 \equiv D_v$ и $x_8 = x_v = H(D_v)$).

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.

На фиг. 1 показана партия из восьми маркированных оригинальных изделий A_1, ..., A_8, каждое из которых имеет соответствующую защитную маркировку 110, нанесенную на него, и проиллюстрирован способ защиты изделий и соответственных связанных с изделием цифровых данных D1, ..., D8 посредством дерева цифровых подписей изделий. Деревья, связанные с цифровыми подписями, хорошо известны

(двоичные хеш-деревья, n-арные хеш-деревья или деревья Меркла), они обычно имеют базовые узлы или листовые узлы, которые используются для создания узлов следующего (промежуточного) уровня путем цифрового подписывания конкатенации цифровых подписей, связанных с листовыми узлами согласно определенной упорядоченности листовых узлов. В случае двоичного дерева цифровые подписи, связанные с узлами первого промежуточного уровня, соответственно вычисляют путем цифрового подписывания (например, с помощью односторонней хеш-функции H или односторонней функции эллиптической кривой и т.д.) конкатенации цифровых подписей, связанных с двумя последовательными листовыми узлами. В случае n-арного дерева значения узлов первого промежуточного уровня получают путем конкатенации значений n последовательных листовых узлов. Дерево также может иметь более сложную структуру (смешанные деревья), так как конкатенацию листовых узлов можно осуществлять парами последовательных узлов для определенных листовых узлов, тройкой узлов для других последовательных листовых узлов и т.д. Из соображений упрощения простое двоичное дерево с восемью листовыми узлами показано на фиг. 1: соответственные значения восьми листовых узлов a(1,1), ..., a(1,8) дерева, соответственно, соответствуют цифровым подписям изделия $x_1 = H(D_1)$, ..., $x_8 = H(D_8)$. Значение первого индекса, т.е. "1", для всех листовых узлов указывает первый уровень (или базовый уровень) дерева, а второй индекс, идущий от 1 до 8, указывает упорядоченность (листовых) узлов дерева. Значения узлов (не листовых) следующего уровня, т.е. четырех узлов второго уровня a(2,1), a(2,2), a(2,3) и a(2,4), получают путем цифрового подписывания конкатенации (символически представленной оператором "+"), в данном случае посредством хеш-функции, значений пар листовых узлов, т.е. пар их дочерних узлов в дереве. Эта группировка дочерних узлов для получения значений узлов следующего уровня определяет упорядоченность конкатенации дерева. Для упрощения обозначений используют символ узла a(i,j), чтобы также представлять связанное с ним значение (т.е. связанную с ним цифровую подпись). В данном случае дерево имеет только два промежуточных уровня выше уровня листовых узлов и корневой узел на верхнем уровне. Уровень корневого узла фактически является последним уровнем узла, отличного от листового, дерева. Таким образом, значения четырех узлов, отличных от листовых, следующего промежуточного уровня представляют собой

a(2,1) = H(a(1,1)+a(1,2)), т.е. $a(2,1) = H(H(D_1)+ H(H(D_2))$, (где a(1,1) и a(1,2) представляют собой дочерние узлы узла a(2,1)),

a(2,2) = H(a(1,3)+a(1,4)),

a(2,3) = H(a(1,5)+a(1,6)),

a(2,4) = H(a(1,7)+a(1,8))

и для следующего, предпоследнего, уровня узлов (в данном случае третьего уровня) представлены два значения узлов

a(3,1) = H(a(2,1)+a(2,2)),

a(3,2) = H(a(2,3)+a(2,4)).

Отметим, что для каждого узла, отличного от листового, можно выбрать другую упорядоченность конкатенации дерева, например, вместо того, чтобы иметь a(2,4) = H(a(1,7)+a(1,8)), определим, что a(2,4) = H(a(1,8)+a(1,7)), что дает другое значение узла.

Наконец, значение корневого узла R дерева или контрольную корневую цифровую подпись получают как R = H(a(3,1)+a(3,2)).

Из-за каскада конкатенаций, задействованных в дереве, практически невозможно получить корневое значение, если какой-либо бит цифровых данных изменяется в узле (в частности, в листовом узле). Более того, если в партию включены некоторые виртуальные изделия (цифровые данные виртуальных изделий которых известны только системе, создающей цифровые подписи листовых узлов дерева), фальшивомонетчик не сможет получить корневую цифровую подпись, даже зная цифровые данные всех произведенных (и маркированных) изделий партии.

Согласно настоящему изобретению контрольная корневая цифровая подпись R 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 корневой базе данных, открытой для пользователя, или в предпочтительном варианте - ее хранения в блокчейне (или в базе данных, защищенной блокчейном), открытом для пользователя. Затем пользователь может сохранить контрольное значение R, полученное из этих доступных источников.

Для каждого изделия A_i партии соответствующий ключ верификации изделия k_i (или путь верификации) связанного дерева затем вычисляют как последовательность соответственных цифровых подписей, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел, соответствующий цифровой подписи изделия, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне. В примере фиг. 1 представлены восемь ключей верификации k_1, ..., k_8, соответственно, соответствующих восьми изделиям A_1, ..., A_8 партии и их соответствующим восьми листовым узлам a(1,1), ..., a(1,8):

1) для листового узла $a(1,1)=x_1 = H(D_1)$, соответствующего изделию A_1, ключ верификации представляет собой $k_1=\{a(1,2),a(2,2),a(3,2)\}$, из которого можно извлечь значение корневой цифровой подписи R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из листового узла $a(1,1)=x_1$ и листового узла $a(1,2)=x_2$ в k_1 ($a(1,2)$ представляет собой другой листовой узел, имеющий такой же родительский узел, т.е. узел $a(2,1)$, что и листовой узел, соответствующий цифровой подписи изделия x_1, т.е. узел $a(1,1)$), получают значение родительского узла $a(2,1)$ посредством $a(2,1) = H(a(1,1)+a(1,2))$ (т.е. $a(2,1) = H(x_1+x_2)$),

ii) из полученного $a(2,1)$ и значения следующего узла в k_1, т.е. $a(2,2)$ следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т.е. узел $a(3,1)$, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т.е. узел $a(2,1)$, получают значение родительского узла $a(3,1)$ посредством $a(3,1) = H(a(2,1)+a(2,2))$,

iii) из полученного $a(3,1)$ и значения следующего узла в k_1, т.е. $a(3,2)$ предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т.е. корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т.е. узел $a(3,1)$, получают значение корневого узла R посредством $R = H(a(3,1)+a(3,2))$.

Примечание: в этом примере представлено три этапа i), ii) и iii), поскольку дерево имеет три уровня ниже уровня корневых узлов и, таким образом, ключ верификации содержит три значения узлов.

Таким образом, значение корневого узла дерева можно получить как

$R = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))$.

2) для листового узла $a(1,2)=x_2=H(D_2)$, соответствующего изделию A_2, ключ верификации представляет собой $k_2=\{a(1,1),a(2,2),a(3,2)\}$, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,2)=x_2$ и $a(1,1)=x_1$ в k_1 ($a(1,1)$ представляет собой другой листовой узел, имеющий такой же родительский узел, т.е. узел $a(2,1)$, что и листовой узел, соответствующий цифровой подписи изделия x_2, т.е. узел $a(1,2)$), получают значение родительского узла $a(2,1)$ посредством $a(2,1) = H(a(1,1)+a(1,2))$,

ii) из полученного $a(2,1)$ и значения следующего узла в k_2, т.е. $a(2,2)$ следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т.е. узел $a(3,1)$, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т.е. узел $a(2,1)$, получают значение родительского узла $a(3,1)$ посредством $a(3,1) = H(a(2,1)+a(2,2))$,

iii) из полученного $a(3,1)$ и значения следующего узла в k_2, т.е. $a(3,2)$ предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т.е. корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т.е. узел $a(3,1)$, получают значение корневого узла R посредством $R = H(a(3,1)+a(3,2))$.

Таким образом, значение корневого узла дерева можно получить как

$R = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2))$.

3) для листового узла $a(1,3)=x_3=H(D_3)$, соответствующего изделию A_3, ключ верификации представляет собой $k_3=\{a(1,4),a(2,1),a(3,2)\}$, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,3)= x_3$ и $a(1,4) = x_4$ в k_3 ($a(1,4)$ представляет собой другой листовой узел, имеющий такой же родительский узел, т.е. узел $a(2,2)$, что и листовой узел, соответствующий цифровой подписи изделия x_3, т.е. узел $a(1,3)$), получают значение родительского узла $a(2,2)$ посредством $a(2,2) = H(a(1,3)+a(1,4))$,

ii) из полученного $a(2,2)$ и значения следующего узла в k_3, т.е. $a(2,1)$ следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т.е. узел $a(3,1)$, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т.е. узел $a(2,2)$, получают значение родительского узла $a(3,1)$ посредством $a(3,1) = H(a(2,1)+a(2,2))$,

iii) из полученного $a(3,1)$ и значения следующего узла в k_3, т.е. $a(3,2)$ предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, т.е. корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, т.е. узел $a(3,1)$, получают значение корневого узла R посредством $R = H(a(3,1)+a(3,2))$.

Таким образом, значение корневого узла дерева можно получить как

$R = H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2))$.

4) для листового узла $a(1,4) = x_4 = H(D_4)$, соответствующего изделию A_4, ключ верификации представляет собой $k_4 = \{a(1,3),a(2,1),a(3,2)\}$, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,4) = x_4$ и $a(1,3) = x_3$ в k_4 получают значение родительского узла $a(2,2)$ посредством $a(2,2) =$

H(a(1,3)+a(1,4)),

ii) из полученного a(2,2) и значения следующего узла в k_4, т.е. a(2,1) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,1) посредством a(3,1) = H(a(2,1)+a(2,2)),

iii) из полученного a(3,1) и значения следующего узла в k_4, т.е. a(3,2) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить как

R = H(H(a(2,1)+H(a(1,3)+a(1,4)))+a(3,2)).

5) для узла $a(1,5) = x_5 = H(D_5)$, соответствующего изделию A_5, ключ верификации представляет собой k_5 = {a(1,6),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,5) = x_5$ и $a(1,6) = x_6$ в k_5 получают значение родительского узла a(2,3) посредством a(2,3) = H(a(1,5)+a(1,6)),

ii) из полученного a(2,3) и значения следующего узла в k_5, т.е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = a(3,2) = H(a(2,3)+a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в k_5, т.е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить как

R = H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4))).

6) для узла $a(1,6) = x_6 = H(D_6)$, соответствующего изделию A_6, ключ верификации представляет собой k_6 = {a(1,5),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,6) = x_6$ и $a(1,5) = x_5$ в k_6 получают значение родительского узла a(2,3) посредством a(2,3) = H(a(1,5)+a(1,6)),

ii) из полученного a(2,3) и значения следующего узла в k_6, т.е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = a(3,2) = H(a(2,3)+a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в k_6, т.е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить как

R = H(a(3,1)+H(H(a(1,5)+a(1,6))+a(2,4))).

7) для узла $a(1,7) = x_7 = H(D_7)$, соответствующего изделию A_7, ключ верификации представляет собой k_7 = {a(1,8),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,7) = x_7$ и $a(1,8) = x_8$ в k_7 получают значение родительского узла a(2,4) посредством a(2,4) = H(a(1,7)+a(1,8)),

ii) из полученного a(2,4) и значения следующего узла в k_7, т.е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3)+a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в k_7, т.е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить как

R = H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8)))).

8) для узла $a(1,8) = x_8 = H(D_8)$, соответствующего изделию A_8, ключ верификации представляет собой k_8 = {a(1,7),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполненных согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из $a(1,8) = x_8$ и $a(1,7) = x_7$ в k_8 получают значение родительского узла a(2,4) посредством a(2,4) = H(a(1,7)+a(1,8)),

ii) из полученного a(2,4) и значения следующего узла в k_8, т.е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3)+a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в k_8, т.е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1)+a(3,2)).

Таким образом, значение корневого узла дерева можно получить как

R = H(a(3,1)+H(a(2,3)+H(a(1,7)+a(1,8)))).

Как правило, для извлечения (потенциального) значения корневого узла, начиная с заданного значения листового узла и значений узлов, определенных в ключе верификации, связанном с указанным заданным листовым узлом, осуществляют следующие этапы:

извлечения из последовательности значений узлов в ключе верификации значения (т.е. значения цифровой подписи) каждого другого листового узла дерева, имеющего такой же родительский узел, что

и у заданного листового узла, и вычисления цифровой подписи конкатенации заданного значения узла и, соответственно, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, извлеченного значения указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла заданного листового узла;

последовательно на каждом следующем уровне в дереве и до предпоследнего уровня узлов

извлечения из последовательности значений узлов в ключе верификации значения каждого другого узла, отличного от листового, дерева, имеющего такой же родительский узел, что и у предыдущего такого же родительского узла, рассмотренного на предшествующем этапе, и

вычисления цифровой подписи конкатенации значения указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая значение указанного такого же родительского узла указанного предыдущего такого же родительского узла; и

вычисления цифровой подписи конкатенации полученных значений узлов, отличных от листовых, соответствующих предпоследнему уровню узлов дерева согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая корневую цифровую подпись корневого узла дерева.

Как ясно из вышеуказанного примера, значение корневого узла R можно наконец извлечь из любого заданного значения листового узла посредством цифровой подписи конкатенации этого значения листового узла только со значениями узлов, определенными в соответствующем ключе верификации. Таким образом, объем данных в информации о верификации, который необходим для извлечения значения корневого узла, явно намного меньше, чем объем данных, необходимый для вычисления контрольного значения корневого узла (т.е. на основании только значений листовых узлов путем вычисления всех значений узлов, отличных от листовых, промежуточных уровней дерева): это преимущество настоящего изобретения с учетом ограничения ограниченного размера, доступного для защитной маркировки (например, двухмерного штрих-кода).

Согласно настоящему изобретению защитная маркировка 110 (возможно, защищенная от несанкционированного доступа), нанесенная на изделие A_i партии изделий, включает информацию о верификации V_i, что обеспечивает операции как проверки в режиме "онлайн", так и автономной проверки аутентичности маркированного изделия, соответствия связанных с ним данных относительно данных подлинного маркированного изделия, или даже соответствия изображения изделия относительно изображения подлинного маркированного изделия, путем обеспечения уникальной, неизменной и защищенной от подделки связи между данными изделия D_i и принадлежностью маркированного изделия A_i к заданной партии подлинных изделий, сохраняя при этом размер в битах цифрового представления этой информации о верификации V_i на уровне, совместимом с содержимым данных двухмерного машиночитаемого штрих-кода, который можно легко считывать посредством обычного считывателя: эта информация о верификации содержит цифровые данные изделия D_i и соответствующий ключ верификации k_i, $V_i = (D_i,k_i)$. Операции проверки включают извлечение значения партии или контрольной корневой цифровой подписи R дерева, связанного с партией, путем первого считывания цифровых данных изделия D_i и соответствующего ключа верификации k_i на машиночитаемой защитной маркировке 110 (или на изображении защитной маркировки) на изделии A_i (соответственно, на изображении A_i), затем вычисление потенциальной цифровой подписи изделия X_i посредством односторонней функции считанных цифровых данных изделия D_i как $X_i = H(D_i)$, и вычисление потенциальной корневой цифровой подписи R^c, как раскрыто выше, из цифровой подписи конкатенации X_i и значений узлов дерева согласно последовательности значений узлов, указанных в ключе верификации k_i. Эта схема защиты, преимущество которой заключается в том, что нет необходимости в шифровании данных и, следовательно, управлении ключами шифрования/дешифрования (в частности, криптографический ключ не включен в защитную маркировку), является гораздо более надежной в отношении криптоаналитической атаки по сравнению с обычным шифрованием данных с помощью открытого ключа шифрования - личного ключа дешифрования (например, системы RSA "Ривест-Шамир-Адлеман"). В результате размер цифровых данных, которые должны быть представлены в защитной маркировке согласно настоящему изобретению, является компактным и позволяет использовать обычные двухмерные штрих-коды (например, QR-код) и, следовательно, обычные считыватели штрих-кодов (или даже простой запрограммированный смартфон, имеющий камеру), обеспечивая при этом очень высокий уровень надежности относительно криптоаналитических атак. Более того, эта защитная маркировка совместима как с проверкой в режиме "онлайн" (через сервер, связывающийся со считывателем кода), так и с автономной (через запрограммированный считыватель кода) проверкой аутентичности маркированного изделия и соответствия его данных относительно данных подлинного изделия. Кроме того, согласно настоящему изобретению представление цифровых данных D_i и представление данных ключа k_i могут отличаться, схема конкатенации данных и/или односторонняя функция могут зависеть от уровня узла в дереве, что обеспечивает дополнительные уровни надежности в отношении криптоаналитических атак.

Предпочтительно, чтобы дополнительно уменьшить размер цифровых данных (т.е. информацию о

верификации V), которые должны быть включены в защитную маркировку, если цифровые данные D_i соответственных оригинальных изделий A_i партии распределены между заданными полями, которые являются общими для всех изделий партии, цифровые данные, относящиеся к этим полям, не включены в каждые цифровые данные изделия D_i, но сгруппированы в отдельном блоке данных полей FDB, связанном с партией изделий, и

цифровую подпись x_i оригинального изделия A_i партии затем вычисляют с помощью односторонней функции H конкатенации соответствующих цифровых данных изделия D_i и цифровых данных блока данных полей FDB, т.е. $x_i = H(D_i+FDB)$; и

контрольную корневую цифровую подпись R предоставляют в распоряжение пользователя вместе со связанным блоком данных полей FDB (что также обеспечивает неизменность блока данных полей).

В варианте настоящего изобретения блок данных полей FDB независимо предоставляет в распоряжение пользователя контрольную корневую цифровую подпись.

Вышеуказанное уменьшение размера возможно в большинстве случаев, так как большинство данных, связанных с изделиями партии, классифицируются согласно некоторым полям для структурирования данных, например, для фармацевтического продукта обозначения "серийный номер", "данные об истечении срока годности" и т.д., в D_i включаются только данные, связанные с этими полями (например, 12603, май 2020 г. и т.д.), в то время как общие названия полей "серийный номер", "данные об истечении срока годности" и т.д. включены в блок данных полей FDB.

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", т.е. 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
110	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 односторонняя функция H: 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, неко-

торые 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 предпочтительному режиму настоящего изобретения выбран следующий тип функции - односторонняя хеш-функция семейства SHA-2.

Модуль вычисления (не показан) предпочтительно включен в систему защиты для выполнения кода, предусмотренного для осуществления вычислений для цифрового подписывания цифровых данных изделий партии для определения ключей верификации для разных изделий и для вычисления контрольной корневой цифровой подписи соответствующего дерева. Система защиты может также включать подходящие модули для ввода (запрограммированных) значений, соответствующих цифровым данным D_v виртуального(ых) изделия(й) A_v. Также можно было бы осуществлять вычисления хеширования, связанные с изделиями, извне (например, на подключенном удаленном сервере), например, где бы ни изготовлялись изделия, чтобы избежать необходимости передавать необработанные данные изделия D_i по сети с этого сайта (или сайтов) к системе защиты, если есть проблема.

Для каждого изделия A_i компилируется соответствующая информация о верификации V_i, которая кодируется (предоставляется) 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 магнитночитаемой 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 $V_v = (D_v,k_v)$ может быть связана с ним внутри системой 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: т.е. $V_i = (D_i,k_i)$.

Дополнительные данные изделия могут дополнительно быть связаны с изделием и могут включать, например, значение партии, т.е. контрольную корневую цифровую подпись R или любую другую информацию, которую разработчик системы (или администратор системы) выбирает включить, как, например, связанный с товаром серийный номер, 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, номер 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 (т.е. посредством кодирования или любого выбранного представления данных) вместе с соответствующими цифровыми данными изделия D_i в машиночитаемую защитную маркировку 110 изделия, нанесенную на изделие A_i, полученное в результате маркированное оригинальное изделие и связанные с ним данные изделия действительно защищены от подделки и фальсификации.

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 110 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 односторонняя функция H() (например, хеш SHA-256), а затем выполнить операцию $x_1=H(D_1)$ для получения полных данных (x_1,k_1), необходимых для вычисления соответствующей потенциальной корневой цифровой подписи R^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 корневую цифровую подпись R^c, пользователю необходимо дополнительно знать тип схемы конкатенации данных (для конкатенации значений узлов через H(a(i,j)+a(i,k)), которая используется для следующего: пользователь может принимать эту информацию любым способом, либо защищенным (например, используя пару открытого и личного ключей), либо просто запрашивая эту информацию от поставщика изделия или любого другого лица, создавшего данные верификации, либо запрограммировав ее в блоке обработки пользователя. Однако схема конкатенации может фактически соответствовать простому обычному сквозному соединению двух блоков цифровых данных, соответственно, соответствующих значениям двух узлов: в этом случае пользователю не должна передаваться никакая конкретная схема. В некоторых вариантах схема конкатенации может до-

полнительно вставлять блок конкатенации, который может содержать данные, определенные для позиции или уровня конкатенированных блоков цифровых данных в дереве, в результате чего еще более затрудняется криптоаналитическая атака.

Зная схему конкатенации данных, пользователь может затем вычислить (например, посредством запрограммированного подходящим образом устройства для формирования изображения) потенциальную корневую цифровую подпись R^c, как раскрыто выше, путем пошагового цифрового подписывания конкатенации цифровой подписи изделия x_1 и значений узлов согласно последовательности узлов, определенных в ключе верификации k_1, см. выше п.1), относящийся к узлу a(1,1), выполненный согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева. В данном случае потенциальную корневую цифровую подпись получают как (упорядоченность узлов в дереве задается соответственными индексами (i,j) уровня и позиции на уровне)

$$R^c = H(H(H(a(1,1)+a(1,2))+a(2,2))+a(3,2)).$$

Эта вычисленная потенциальная корневая цифровая подпись R^c затем должна быть равна доступному (или опубликованному) контрольному значению R: 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 R^c и доступных контрольных корневых цифровых подписей R 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 корневых цифровых подписей может указать пользователю, что изделие, вероятно, является аутентичным. Это особенно интересно, потому что для аутентификации изделия A_1 нет необходимости в аутентификации его материала, т.е. посредством внутренней физической характеристики A_1 или посредством конкретной защитной маркировки на основе материала, нанесенной на A_1.

Ссылка для доступа к контрольной корневой цифровой подписи R для партии, соответствующей изделию A_1, может быть включена в защитную маркировку 110 (например, веб-адрес, если R можно извлечь из соответствующего веб-сайта), хотя это не предпочтительный вариант.

В некоторых реализациях получатели изделия A_i могут иметь возможность "визуально" извлекать данные изделия, соответствующие цифровым данным изделия D_i, непосредственно из изделия. Например, данные изделия могут быть текстовыми, такими как серийный номер или текст в описательном письме, или являться некоторой 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 и R^c, а также сравнить данное значение с доступным контрольным значением партии R, как раскрыто выше.

Предпочтительно контрольная корневая цифровая подпись (т.е. значение партии) R хранится в доступной для поиска корневой базе данных, к которой может получить доступ (через канал связи) пользователь с помощью своего устройства для формирования изображения, оснащенного блоком связи, как это имеет место с вышеуказанным примером смартфона. Пользователь, которому необходимо верифицировать изделие A_1, может просто отправить корневой запрос со своего смартфона на адрес базы данных через интерфейс доступа к базе 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 контрольное значение партии R, а интерфейс доступа вернет контрольную корневую цифровую подпись R на смартфон. База данных может быть защищена блокчейном, чтобы усилить неизменность сохраненных корневых цифровых подписей. Преимущество настоящего изобретения заключается в том, чтобы установить связь между физическим объектом, т.е. оригинальным изделием и его атрибутами, т.е. связанными с изделием данными и его принадлежностью к определенной партии изделий, практически неизменно посредством соответствующей корневой 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, например, 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 ото-

бражаемая информация данным изделия на маркировке данных изделия.

В предпочтительном варианте осуществления данные изделия или его соответствующие цифровые данные изделия D_i дополнительно включают (уникальные) характеристические цифровые данные (CDD) уникальной физической характеристики маркированного оригинального изделия A_i, что можно использовать для (материальной) аутентификации A_i. Таким образом, с помощью характеристических цифровых данных, соответствующих физической характеристике изделия A_i, представляющих собой CDD_i, соответствующие данные уникальной физической подписи UPS_i можно получить путем кодирования CDD_i (предпочтительно посредством односторонней функции): например, взяв хеш-значение цифровых данных CDD_i, т.е. $UPS_i = H(CDD_i)$. 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 характеристических цифровых данных CDD_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, $UPS_i = H(CDD_i)$. Характеристические цифровые данные CDD_i, которые генерировали подпись UPS_i, представляют собой контрольные характеристические цифровые данные для A_i, и полученная подпись UPS_i представляет собой соответствующие контрольные данные физической подписи для A_i. Предпочтительно UPS_i, т.е. 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 CDD_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 характеристических цифровых данных CDD_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 характеристическими цифровыми данными CDD_i, сохраненными в памяти устройства для формирования изображения: в случае совпадения $CDD_i = CDD_i^c$, изделие A_i считается подлинным (его цифровое содержимое соответствует содержимому подлинного маркированного оригинального изделия). Если контрольные характеристические цифровые данные CDD_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 CDD_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 CDD_i^c UPC_i^c, извлеченных из цифровых данных D_i, т.е. $UPS_i^c = H(CDD_i^c)$, 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 характеристических цифровых данных CDD_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 CDD_i^c с копией контрольных CDD_i (сохраненных в памяти устройства для формирования изображения): в случае "обоснованного" совпадения $CDD_i^c \approx CDD_i$ (т.е. 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 CDD_i, сохраненных в памяти устройства для формирования изображения в виде $UPS_i^c = H(CDD_i)$, 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 контрольного значения партии R из считанной информации о верификации (D_i,k_i) на защитной маркировке на A_i. В предпочтительном режиме копия контрольных характеристических цифровых данных $(CDD)_i$, вместо того, чтобы храниться в памяти устрой-

ства 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 характеристических цифровых данных CDD_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 CDD_i и/или UPS_i 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 характеристических цифровых данных CDD_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 возбуждения 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 блоком обработки 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 $\tau_c \approx \tau$ (в заданном диапазоне отклонения). В данном случае цифровые данные CDD_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 вышеуказанных примеров, технический результат включения контрольных характеристических цифровых данных в информацию о верификации защитной маркировки заключается в обеспечении защищенной от подделки связи между цифровыми данными изделия и данными (материальной) аутентификации этого конкретного изделия.

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

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 (т.е. набор возможных ключей) больше, чем ее диапазон (т.е. 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, т.е. видимые напечатанные данные, такие как название доку-

мента 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 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, т.е. 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 $\mu = 1024$) связанные цифровые данные D_j паспорта включают цифровые данные, соответствующие вышеупомянутым данным 230a-230e.

В варианте осуществления связанные с паспортом цифровые данные D_j могут включать только значения полей, которые являются общими для всех доставленных паспортов, в то время как поля в целом, т.е. "Паспорт", "Фамилия", "Пол", "Дата рождения", "Гражданство", "Место проживания", "Место рождения", "Дата выдачи паспорта" и "Период окончания срока действия" включены в отдельный блок данных полей FDB, как раскрыто выше: например, D_1 только содержит представление значений полей "Доу", "Джон", "М", "20 марта 1975 г.", "США", "Де-Мойн", "Окленд", "24 февраля 2018 г." и "23 февраля 2020 г.".

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.

Для всех подписей паспортов в партии контрольную корневую цифровую подпись R вычисляют согласно упорядоченности дерева и упорядоченности конкатенации дерева связанного (двоичного) дерева, как раскрыто выше. Поскольку в партии $\mu = 1024$ паспортов, соответствующее двоичное дерево имеет 1024 листовых узла a(1,1) ,..., a(1024) для первого уровня, 512 узлов, отличных от листовых, a(2,1), ..., a(2,512) для второго уровня, 256 узлов, отличных от листовых, a(3,1), ..., a(3,256) для третьего уровня и т.д., вверх до предпоследнего уровня узлов (в данном случае уровня 10) с узлами, отличными от листовых, a(10,1) и a(10,2), и верхний узел, соответствующий корневому узлу R (уровень 11 дерева). Значения листовых узлов представляют собой $a(1,j) = x_j = H(D_j)$, j=1, ..., 1024, значения узлов второго уровня представляют собой a(2,1) = H(a(1,1)+a(1,2)), ..., a(2,512) = H(a(1,1023)+a(1,1024)), и т.д., и контрольная корневая цифровая подпись R представляет собой R = H(a(10,1)+a(10,2)). Таким образом, каждый ключ верификации k_j представляет собой последовательность из 10 значений узлов. Защитная маркировка 210, нанесенная на паспорт A_j, включает цифровые данные паспорта D_j и соответствующий ключ верификации k_j (т.е. информацию о верификации $V_j = (D_j,k_j)$).

Для операции проверки действительного соответствия цифровых данных паспорта D_j и ключа верификации k_j в защитной маркировке 210 биометрического паспорта A_j данным подлинного биометриче-

ского паспорта, принадлежащего к партии μ биометрических паспортов, имеющей значение партии R, необходимо только вычисление цифровой подписи паспорта $x_j = H(D_j)$ и верификация того, что x_j и ключ верификации k_j обеспечивают извлечение доступной соответствующей контрольной корневой цифровой подписи R посредством 10-кратного составления (в данном случае дерево имеет десять уровней ниже корневого уровня) хеш-функции конкатенации значения узла a(1,j) и значений узлов в k_j (согласно упорядоченности узлов в двоичном дереве и упорядоченности конкатенации дерева с обычной схемой конкатенации). 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 A_1, содержит информацию о верификации (D_1,k_1), с цифровыми данными паспорта D_1, соответствующими напечатанным данным 230a-230d паспорта, биометрическим данным 230e и уникальному серийному номеру 235, и ключом верификации k_1, соответствующим последовательности из 10 значений узлов {a(1,2),a(2,2),...,a(10,2)}, которые необходимы для извлечения корневого значения R из значения узла a(1,1) паспорта A_1 (где $a(1,1) = x_1 = H(D_1)$). Контрольной корневой цифровой подписи R можно 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) корневых цифровых подписей всех доставленных партий биометрических паспортов. В примере, показанном на фиг. 2B, информационная база 250 данных является локальной (т.е. 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, т.е. 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 конкатенацией значений узлов), запущенное на компьютере 290, вычисляет цифровую подпись паспорта x_1 (как $x_1=H(D_1)$ и потенциальное значение партии R^c как

$$H(H(H(H(H(H(H(H(H(a(1,1)+a(1,2))+a(2,2))+..)+..)+..)+..)+..)+..)+a(9,2))+a(10,2)),$$

т.е. 10-кратного составления хеш-функции конкатенации значения узла a(1,1) и значений узлов в k_1={a(1,2),a(2,2),...,a(10,2)}. Затем компьютер может, например, выполнить поиск в локальной информационной базе 250 данных контрольной корневой цифровой подписи R, совпадающей с контрольным значением R^c: в случае несовпадения паспорт является поддельным и "Джон Доу" (т.е. проверяемый человек, утверждающий, что его зовут Джон Доу) может быть арестован. В случае совпадения R^c с некоторой сохраненной контрольной корневой цифровой подписью, паспорт считается подлинным, и сотрудник может выполнить дополнительные проверки безопасности:

сотрудник извлекает цифровую фотографию 255 личности, сохраненную 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 (т.е. лицо Джона Доу) с лицом проверяемого человека и оценить, похожи ли эти два лица или нет; и

сотрудник извлекает биометрические данные 230e на 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 соответствующие биометрические данные человека: сотрудник затем проверяет посредством программы, запущенной на компьютере 290, сходны ли извлеченные биометриче-

ские данные 230e (в пределах заданной погрешности) с полученными биометрическими данными человека.

Если два лица и биометрические данные считаются сходными, все в порядке, и проверяемый человек действительно является реальным 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 k. 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, т.е. каждый разрешенный компонент самолета для установки или ремонта на данном самолете, имеет соответствующий идентификационный документ компонента самолета AC-ID, который содержит такие же 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 подписью 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 μ 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}, установленным на самолете HB-SNO. На фиг. 3, в частности, показан компонент A_{125} партии 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:A_{125}: 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 $x_{125} = H(D_{125})x_{125} = H(D_{125})$. 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, ..., μ). Согласно настоящему изобретению дерево, связанное с партией компонентов (в данном случае двоичное дерево), построено с μ листовых узлов a(1,1), ..., a(1,μ), соответственно, соответствующих μ цифровых подписей компонентов x_1, ..., x_μ соответственных цифровых данных компонента D_1, ..., D_μ идентификационных документов AC-ID:A_1, ..., AC-ID:A_μ компонентов A_1, ..., A_μ. В данном случае упорядоченность узлов двоичного дерева является обычной упорядоченностью, т.е. узлы a(i,j) расположены согласно значениям индексов (i,j): индекс i указывает уровень в дереве, начиная от уровня листовых узлов (i=1) до предпоследнего уровня узлов ниже корневого узла, и индекс j, проходящий от 1 до μ для уровня листовых узлов (уровень 1), от 1 до μ/2 для следующего уровня узлов (отличных от листовых) (уровень 2), и т.д. и от 1 до 2 для предпоследнего уровня узлов. Дерево, содержащее уровни узлов, начиная от листовых узлов до корневого узла, при этом каждый узел, отличный от листового, дерева соответствует цифровой подписи посредством односторонней функции H конкатенации соответственных цифровых подписей его дочерних узлов согласно упорядоченности конкатенации дерева.

Контрольную корневую цифровую подпись R для партии μ компонентов самолета A_1, ..., A_μ вычисляют посредством односторонней функции (обычной) конкатенации корневых значений дерева (как раскрыто ниже). Контрольную корневую цифровую подпись R затем сохраняют в доступной для поиска базе данных (предпочтительно, блокчейн), открытой для специалистов, ответственных за контроль или замену установленных компонентов. Таким образом, дерево содержит уровни узлов, начиная от листовых узлов до корневого узла дерева, при этом каждый узел, отличный от листового, дерева соответствует цифровой подписи посредством односторонней функции H конкатенации соответственных цифровых подписей его (двух) дочерних узлов согласно упорядоченности конкатенации дерева (в данном случае обычной), корневой узел соответствует контрольной корневой цифровой подписи R, т.е. цифровой подписи посредством односторонней функции H конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве (согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева).

Для заданного компонента A_i партии ключ верификации k_i, соответствующий цифровой подписи компонента x_i (т.е. листовой узел a(1,i)) цифровых данных компонента D_i, вычисляют как последовательность соответственных цифровых подписей, начиная от уровня листовых узлов до предпоследнего уровня узлов дерева, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел a(1,i), соответствующий цифровой подписи изделия x_i, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне. 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 R. Однако в предпочтительном варианте, обеспечивающем полную автономную проверку, считыватель специалиста подключен к компьютеру, имеющему память, сохраняющую все корневые 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 блоке обработки компьютера, который вычисляет подпись $x_{125}=H(D_{125})$ из считанных цифровых данных D_{125}), вычисления потенциального значения партии R^c посредством односторонней функции H, запрограммированной на блоке обработки компьютера в виде хеш-значения конкатенации значения листового узла $a(1,125)=x_{125}$ и значений узлов, заданных в соответствующем ключе верификации k_{125}, и проверки совпадения потенциального значения партии R^c со значением контрольных корневых цифровых подписей, сохраненных в памяти компьютера (т.е. R, соответствующее самолету HB-SNO). В случае полного совпадения (т.е. совпадения серийных номеров и $R^c = RB^c = B$), компонент A_{125} считается подлинным и принадлежит к (обновленной) партии самолета разрешенных компонентов самолета HB-SNO, в случае несовпадения R^c с сохраненной контрольной корневой цифровой подписью R, или в случае несовпадения серийных номеров, компонент A_{125}, вероятно, является подделкой, или является подлинным компонентом, не разрешенным для самолета HB-SNO (например, 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 аутентичности 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, т.е. характеристическим цифровым данным CDD (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 характеристических цифровых данных CDD, т.е. UPS = H(CDD)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 характеристических цифровых данных CDD^c из измеренной характеристики (например, через специальное приложение, запрограммированное в блоке обработки его компьютера). Затем специалист (или блок обработки его компьютера, если он подходящим образом запрограммирован) сравнивает полученные CDD^c с копией контрольных CDD, сохраненных в памяти компьютера: в случае "обоснованного" совпадения $CDD^c \approx CDD$ (т.е. в пределах некоторого заранее определенного критерия допустимых ошибок) защитная маркировка на основе материала и, следовательно, компонент считаются подлинными.

Как упомянуто выше, копия контрольных характеристических цифровых данные CDD, 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 CDD^c на защитной маркировке и проверить совпадение подписи UPS, сохраненной в памяти компьютера, с потенциальной подписью UPS^c, вычисленной из считанных потенциальных CDD^c путем вычисления $UPS^c = H(CDD^c)$: 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 изображе-

нии 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 R 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 R;

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 R^c (посредством запрограммированной односторонней хеш-функции H) в виде цифровой подписи посредством хеш-функции H конкатенации значения листового узла x_{125} и значений узлов, указанных в ключе верификации k_{125} (согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева); и

верификации совпадения потенциального значения партии R^c с контрольным значением партии R.

Вышеупомянутые операции верификации соответствия также можно осуществлять на простой фотокопии оригинального документа AC-ID:A_{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, относительно 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 mm коробок (или изделий) A_1, ..., 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 характеристических цифровых данных CDD-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 характеристические цифровые данные CDD.

Согласно настоящему изобретению штрих-код 410 коробки A_i ($i \in \{1,...,\mu\}$) партии содержит цифровые данные коробки D_i, соответствующие цифровому представлению вышеупомянутых обычных данных 430a-430g коробки A_i,

соответственных серийных номеров 435 блистерных упаковок 401, содержащихся в коробке A_i, и контрольных цифровых данных уникальной физической характеристики CDD-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 $x_i = H(D_i)$, $i = 1, ..., \mu$.

Дерево, связанное с партией коробок (в данном случае двоичное дерево), построено с μ листовых узлов $a(1,1)$, ..., $a(1,\mu)$, соответственно, соответствующих μ цифровых подписей коробки x_1, ..., x_μ соответственных цифровых данных D_1, ..., D_μ коробок A_1, ..., A_μ. В данном случае упорядоченность узлов

двоичного дерева является обычной упорядоченностью, т.е. узлы a(i,j) расположены согласно значениям индексов (i,j): индекс i указывает уровень в дереве, начиная от уровня листовых узлов (i=1) до предпоследнего уровня узлов ниже корневого узла, и индекс j, проходящий от 1 до μ для уровня листовых узлов (уровень 1), от 1 до μ/2 для следующего уровня узлов (отличных от листовых) (уровень 2), и т.д. и, наконец, от 1 до 2 для предпоследнего уровня узлов. Дерево содержит уровни узлов, начиная от листовых узлов, a(1,1), ..., a(1, μ), до корневого узла, при этом каждый узел, отличный от листового, дерева соответствует цифровой подписи посредством односторонней хеш-функции H конкатенации соответственных цифровых подписей его дочерних узлов согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева (корневой узел соответствует контрольной корневой цифровой подписи).

Контрольную корневую цифровую подпись R для всех коробок партии затем вычисляют посредством односторонней хеш-функции H в виде цифровой подписи конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве (согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева).

Полученная контрольная корневая цифровая подпись R 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 корневой базе данных, 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 корневую базу данных или блокчейн и принять обратно соответствующее контрольное значение партии R. Ссылка для доступа к доступной для поиска корневой базе данных (через Интернет, например) или блокчейну может быть включена в маркировку 440 данных коробки (показанную как QR-код на фиг. 4), напечатанную на коробке A_i. Предпочтительно контрольная корневая цифровая подпись R становится доступной для пользователя локально, так что пользователь может осуществлять операции проверки в автономном режиме (т.е. не имея доступа к удаленным средствам хранения для получения R): 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 блоке обработки смартфона) и память которого сохраняет контрольную корневую цифровую подпись R.

Для каждой коробки A_i партии μ упаковок с лекарственными препаратами есть соответствующий ключ верификации k_i, связанный с цифровой подписью коробки x_i, т.е. с узлом a(1,i), его вычисляют как последовательность соответственных цифровых подписей коробки от уровня листовых узлов до предпоследнего уровня узлов дерева, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел a(1,i), соответствующий цифровой подписи изделия x_i, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне.

Цифровые данные 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 $_i$.

Для верификации аутентичности защищенной коробки A_1 согласно фиг. 4, принадлежащей к партии коробок, имеющих контрольную корневую цифровую подпись R, 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 дополнительно запрограммированное приложение для вычисления подписи с помощью односторонней хеш-функции H и извлечения значения корневого узла из информации о верификации $V_1=(D_1,k_1)$), вычисление соответствующей цифровой подписи коробки x_1 с помощью односторонней функции H как $x_1 = H(D_1)$, получение контрольной корневой цифровой подписи (значения партии) R (в этом примере контрольное значение партии R хранится в памяти считывателя), и проверка совпадения полученной контрольной корневой цифровой подписи R с потенциальной корневой цифровой подписью R^c, полученной из считанной информации о верификации (D_1,k_1) как цифровой подписи посредством односторонней хеш-функции H конкатенации, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, значения листового узла x_1 (листового узла a(1,1)) и значений узлов, указанных в ключе верификации k_1. Если $R^c \neq R$, то коробка A_1 является поддельной. Если $R^c = R$, 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 характеристические цифровые данные CDD^c-A_1, а затем проверить действительную схожесть этих CDD^c-A_1 (в пределах заданной погрешности) с контрольными характеристическими цифровыми данными CDD-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 корневых цифровых подписей (т.е. $R^c = RB^c = B$), 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 (т.е. с $R^c = R$), 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 корневой 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 корневой цифровой подписи с контрольной корневой 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, принадлежащего к партии множества оригинальных изделий, от подделки или фальсификации, при этом каждое оригинальное изделие 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;

формирования дерева на основании множества вычисленных цифровых подписей изделий для оригинальных изделий партии, содержащего узлы, расположенные согласно заданной упорядоченности узлов в дереве, при этом указанное дерево содержит уровни узлов, начиная от листовых узлов, соответствующих множеству цифровых подписей изделий, соответственно, связанных с множеством оригинальных изделий в партии, до корневого узла дерева, каждый узел, отличный от листового, дерева соответствует цифровой подписи посредством односторонней функции конкатенации соответственных цифровых подписей его дочерних узлов согласно упорядоченности конкатенации дерева, корневой узел соответствует контрольной корневой цифровой подписи, т.е. цифровой подписи посредством односторонней функции конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве согласно ука-

занной упорядоченности конкатенации дерева;

связывания с заданным оригинальным изделием соответствующего ключа верификации, представляющего собой последовательность соответственных цифровых подписей, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и листовой узел, соответствующий цифровой подписи заданного оригинального изделия, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне;

предоставления в распоряжение пользователя контрольной корневой цифровой подписи дерева; и

нанесения на заданное оригинальное изделие машиночитаемой защитной маркировки, включающей представление его соответствующих цифровых данных изделия и его соответствующего ключа верификации,

тем самым получая маркированное оригинальное изделие, данные изделия которого защищены от подделки или фальсификации.

2. Способ по п.1, отличающийся тем, что контрольная корневая цифровая подпись корневого узла дерева либо опубликована в среде, открытой для пользователя, либо сохранена в доступной для поиска корневой базе данных, открытой для пользователя, либо сохранена в блокчейне, либо сохранена 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 корневому узлу, маркированные на нем и содержащие информацию, достаточную для обеспечения доступа пользователю к контрольной корневой цифровой подписи корневого узла дерева, соответствующего партии оригинальных изделий, при этом указанная информация является ссылкой в интерфейс доступа, выполненный с возможностью приема от пользователя корневого запроса, содержащего цифровые данные изделия или цифровую подпись цифровых данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно контрольной корневой цифровой подписи соответствующего дерева, при этом интерфейс доступа обеспечивает доступ, соответственно, к одному из следующего:

среда, в которой опубликована контрольная корневая цифровая подпись;

доступная для поиска корневая база данных, в которой сохранена контрольная корневая цифровая подпись; и

блокчейн или, соответственно, база данных, защищенная блокчейном, в котором сохранена контрольная корневая цифровая подпись с временной меткой.

4. Способ по любому из пп.1-3, отличающийся тем, что

виртуальное изделие считается принадлежащим к партии 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 цифровых данных виртуального изделия, указанное виртуальное изделие не создается, а только используется для генерирования связанной с виртуальным изделием цифровой подписи; и

контрольная корневая цифровая подпись, связанная с указанной партией оригинальных изделий, вычислена из дерева, имеющего все цифровые подписи оригинальных изделий партии, включающие цифровую подпись виртуального изделия, в виде листовых узлов.

5. Способ по любому из пп.1-4, отличающийся тем, что

дополнительные цифровые данные изделия, соответствующие цифровым 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 цифровые данные изделия или цифровую подпись цифровых данных изделия, получаемые из защитной маркировки маркированного оригинального изделия, и отправки обратно соответствующих дополнительных цифровых данных изделия.

6. Способ по п.5, отличающийся тем, что дополнительные цифровые данные изделия, соответствующие цифровым данным изделия, связанным с маркированным оригинальным изделием, конкатенированы с указанными цифровыми данными изделия.

7. Способ по любому из пп.1-6, отличающийся тем, что цифровые данные маркированного оригинального изделия включают соответствующие контрольные характеристические цифровые данные уникальной физической характеристики маркированного оригинального изделия или связанного объекта или человека.

8. Способ по п.7, отличающийся тем, что уникальная физическая характеристика маркированного оригинального изделия представляет собой характеристику защитной маркировки на основе материала, нанесенной на оригинальное изделие или на связанный объект.

9. Способ по любому из пп.1-8, отличающийся тем, что в случае распределения цифровых данных соответственных оригинальных изделий партии между заданными полями, общими для всех изделий

партии, и цифровые данные, относящиеся к этим полям, не включены в цифровые данные изделия, но сгруппированы в отдельный блок данных полей, связанный с партией, и при этом

i) цифровую подпись оригинального изделия вычисляют с помощью односторонней функции конкатенации соответствующих цифровых данных изделия и цифровых данных блока данных полей; и

ii) контрольная корневая цифровая подпись поступает в распоряжение пользователя вместе со связанным блоком данных полей.

10. Способ верификации аутентичности изделия или соответствия копии такого изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно способу по любому из пп.1-8, 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, блок обработки с памятью и блок обработки изображения;

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

сохранения в памяти контрольной корневой цифровой подписи корневого узла дерева партии оригинальных изделий и программирования в блоке обработки односторонней функции для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и связанного тестового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления этапов

вычисления с помощью односторонней функции тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей данные изделия на тестовом объекте являются данными подлинного изделия.

11. Способ по п.10, отличающийся тем, что маркированное оригинальное изделие защищено согласно способу по п.9, память блока обработки дополнительно сохраняет связанный блок данных полей, и при этом

этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, включает вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

12. Способ по любому из пп.10 и 11, отличающийся тем, что изделие защищено путем сохранения контрольной корневой цифровой подписи в доступной для поиска корневой базе данных, 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 предварительные этапы

отправки блоком связи посредством канала связи запроса в указанную корневую базу данных и приема обратно контрольной корневой цифровой подписи; и

сохранения принятой корневой цифровой подписи в памяти устройства для формирования изобра-

жения.

13. Способ по любому из пп.10 и 11, отличающийся тем, что изделие защищено согласно способу по п.3, устройство для формирования изображения дополнительно оснащено блоком связи, выполненным с возможностью отправки и приема данных посредством канала связи, при этом способ включает предварительные этапы

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

отправки блоком связи посредством канала связи корневого запроса в указанный интерфейс доступа, содержащего цифровые данные изделия или цифровую подпись указанных цифровых данных изделия, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующей контрольной корневой цифровой подписи связанной партии; и

сохранения принятой контрольной корневой цифровой подписи в памяти устройства для формирования изображения.

14. Способ по любому из пп.10-13, отличающийся тем, что изделие защищено согласно способу по любому из пп.5 и 6, и устройство для формирования изображения дополнительно оснащено средствами связи, выполненными с возможностью отправки в интерфейс информационной базы данных запроса на информацию, содержащего цифровые данные изделия или соответствующие данные цифровой подписи изделия, получаемые из защитной маркировки на тестовом объекте, и приема обратно соответствующих дополнительных цифровых данных изделия.

15. Способ по любому из пп.10-14, отличающийся тем, что изделие защищено согласно способу по любому из пп.7 и 8, и устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики соответственно маркированного оригинального изделия или связанного объекта или человека, и блок обработки запрограммирован для извлечения соответствующих характеристических цифровых данных из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристики соответственно 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 характеристических цифровых данных CDD^c;

сравнения полученных потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD; и

в случае схожести потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD, с заданным критерием допустимого отклонения, субъект считается соответствующим, соответственно, подлинному изделию или объекту или человеку, действительно связанному с подлинным изделием.

16. Способ верификации соответствия цифрового изображения изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно способу по любому из пп.1-8, при этом способ включает этапы

получения цифрового изображения изделия, демонстрирующего защитную маркировку на изделии, посредством устройства для формирования изображения, имеющего блок формирования изображения, блок обработки с памятью и блок обработки изображения;

считывания представления цифровых данных изделия и связанного ключа верификации на полученном цифровом изображении защитной маркировки и извлечения, соответственно, соответствующих тестовых цифровых данных изделия и связанного тестового ключа верификации из указанного считанного представления;

сохранения в памяти контрольной корневой цифровой подписи корневого узла дерева партии оригинальных изделий и программирования в блоке обработки односторонней функции для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и тестового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления этапов

вычисления с помощью односторонней функции тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей цифровое изображение изделия является изображением подлинного маркированного оригинального изделия.

17. Способ по п.16, отличающийся тем, что маркированное оригинальное изделие защищено согласно способу по п.9, память блока обработки дополнительно сохраняет связанный блок данных полей, и при этом

этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, включает вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

18. Способ по любому из пп.16 и 17, отличающийся тем, что оригинальное изделие защищено путем сохранения контрольной корневой цифровой подписи в доступной для поиска корневой базе данных, 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 предварительные этапы

отправки блоком связи посредством канала связи запроса в указанную корневую базу данных и приема обратно контрольной корневой цифровой подписи; и

сохранения принятой корневой цифровой подписи в памяти устройства для формирования изображения.

19. Способ по любому из пп.16-18, отличающийся тем, что оригинальное изделие защищено согласно способу по любому из пп.7 и 8, и устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики, соответственно, объекта или человека, связанного с маркированным оригинальным изделием, и блок обработки запрограммирован для извлечения соответствующих характеристических цифровых данных из сигнала обнаружения, принятого от датчика, устройство для формирования изображения сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике, соответственно, связанного объекта или человека, при этом способ включает дополнительные этапы, при рассматривании субъекта представляющего собой указанный связанный объект или человека:

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

сравнения полученных потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD; и

в случае схожести потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD, с заданным критерием допустимого отклонения, субъект считается соответствующим, соответственно, объекту или человеку, действительно связанному с подлинным маркированным оригинальным изделием.

20. Изделие, принадлежащее 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 свои собственные цифровые данные изделия и соответствующий ключ верификации, указанная партия имеет соответствующую контрольную корневую цифровую подпись, при этом изделие содержит

машиночитаемую защитную маркировку, нанесенную на изделие и включающую представление его цифровых данных изделия и его ключа верификации.

21. Изделие по п.20, отличающееся тем, что цифровые данные изделия включают контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики изделия или связанного объекта или человека.

22. Изделие по п.21, отличающееся тем, что уникальная физическая характеристика изделия представляет собой характеристику защитной маркировки на основе материала, нанесенной на изделие.

23. Система верификации аутентичности изделия или соответствия копии такого изделия относи-

тельно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно способу по любому из пп.1-8, при этом система содержит устройство для формирования изображения, имеющее блок формирования изображения, блок обработки с памятью и блок обработки изображения, при этом память сохраняет контрольную корневую цифровую подпись дерева, соответствующего партии оригинальных изделий, и одностороннюю функцию для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, запрограммированной в блоке обработки, при этом указанная система выполнена с возможностью

получения с помощью устройства для формирования изображения цифрового изображения защитной маркировки на тестовом объекте, представляющем собой указанное изделие или указанную копию изделия;

считывания с помощью устройства для формирования изображения представления цифровых данных изделия и связанного ключа верификации на полученном цифровом изображении защитной маркировки на тестовом объекте и извлечения, соответственно, соответствующих тестовых цифровых данных изделия и тестового ключа верификации из указанного считанного представления;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и связанного ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления на блоке обработки дополнительных запрограммированных этапов

вычисления с помощью односторонней функции тестовой цифровой подписи из вычисленной тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

в результате чего, в случае совпадения указанных корневых цифровых подписей система выполнена с возможностью доставки указания того, что данные изделия на тестовом объекте являются данными подлинного изделия.

24. Система по п.23, отличающаяся тем, что маркированное оригинальное изделие защищено согласно способу по п.9, память блока обработки дополнительно сохраняет связанный блок данных полей, и при этом

этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, включает вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.

25. Система верификации соответствия цифрового изображения изделия относительно маркированного оригинального изделия, принадлежащего к партии оригинальных изделий, защищенных согласно способу по любому из пп.1-8, при этом система содержит устройство для формирования изображения, имеющее блок формирования изображения, блок обработки с памятью и блок обработки изображения, при этом память сохраняет контрольную корневую цифровую подпись дерева, соответствующего партии оригинальных изделий, и одностороннюю функцию для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, запрограммированной в блоке обработки, при этом указанная система выполнена с возможностью

получения цифрового изображения изделия, демонстрирующего защитную маркировку на изделии, посредством устройства для отображения;

считывания с помощью устройства для формирования изображения представления цифровых дан-

ных изделия и связанного ключа верификации на полученном цифровом изображении защитной маркировки и извлечения, соответственно, соответствующих тестовых цифровых данных изделия и связанного тестового ключа верификации из указанного считанного представления;

верификации действительного соответствия извлеченных тестовых цифровых данных изделия и тестового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления на блоке обработки дополнительных запрограммированных этапов

вычисления с помощью односторонней функции тестовой цифровой подписи извлеченных тестовых цифровых данных изделия, при этом указанная тестовая цифровая подпись соответствует тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте;

извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого листового узла тестового дерева, имеющего такой же родительский узел, что и у тестового листового узла, и вычисления цифровой подписи конкатенации тестовой цифровой подписи и извлеченной цифровой подписи указанного каждого другого листового узла, тем самым получая цифровую подпись указанного такого же родительского узла тестового листового узла;

последовательно на каждом следующем уровне в тестовом дереве и до предпоследнего уровня узлов извлечения из последовательности цифровых подписей в тестовом ключе верификации цифровой подписи каждого другого узла, отличного от листового, тестового дерева, имеющего такой же родительский узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем этапе, и вычисления цифровой подписи конкатенации цифровой подписи указанного соответственного каждого другого узла, отличного от листового, и полученной цифровой подписи указанного предыдущего такого же родительского узла, тем самым получая цифровую подпись указанного такого же родительского узла указанного предыдущего такого же родительского узла;

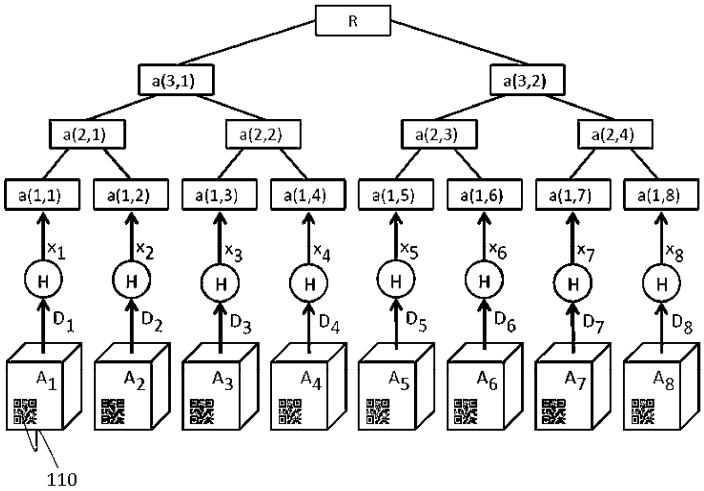
вычисления цифровой подписи конкатенации полученных цифровых подписей узлов, отличных от листовых, соответствующих предпоследнему уровню узлов тестового дерева, тем самым получая потенциальную корневую цифровую подпись корневого узла тестового дерева; и

проверки совпадения полученной потенциальной корневой цифровой подписи с сохраненной контрольной корневой цифровой подписью,

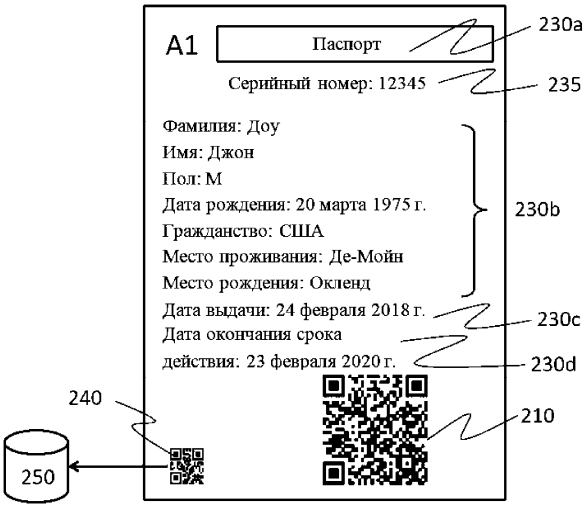
в результате чего, в случае совпадения указанных корневых цифровых подписей система выполнена с возможностью доставки указания того, что цифровое изображение изделия является изображением подлинного маркированного оригинального изделия.

26. Система по п.25, отличающаяся тем, что маркированное оригинальное изделие защищено согласно способу по п.9, память блока обработки дополнительно сохраняет связанный блок данных полей, и при этом

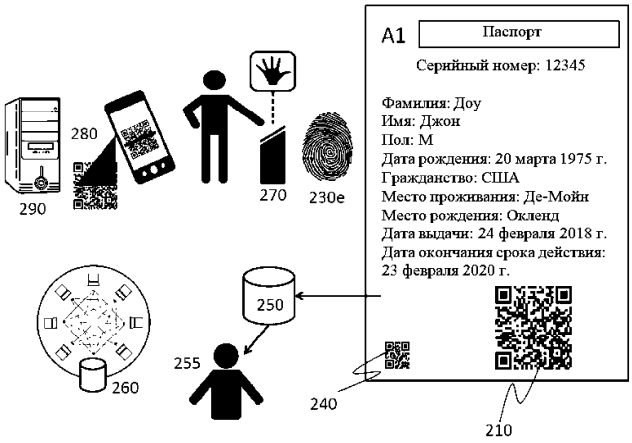
этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем защитной маркировке на тестовом объекте, включает вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных изделия и цифровых данных сохраненного блока данных полей.



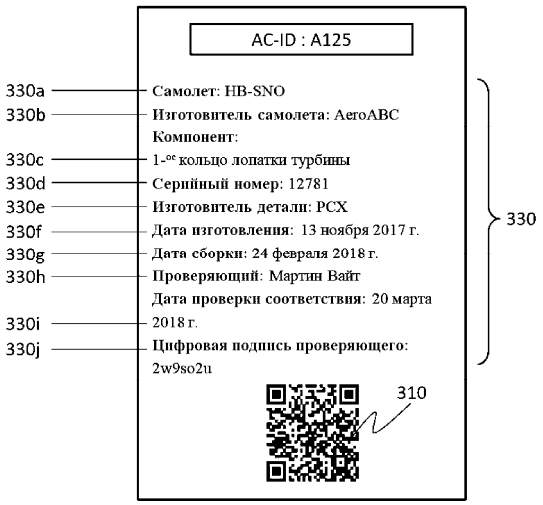
Фиг. 1



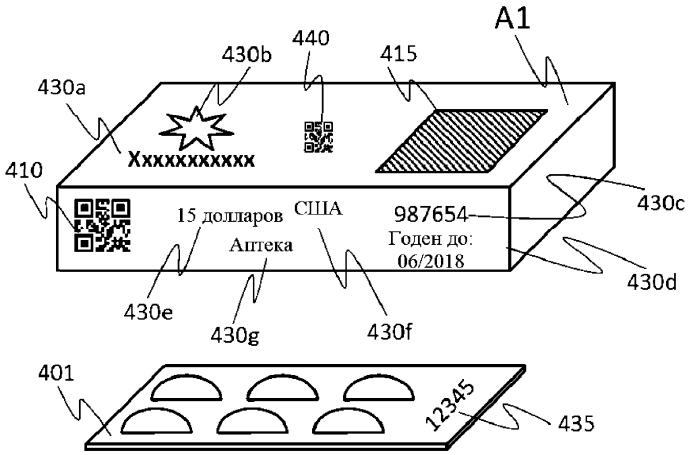
Фиг. 2A



Фиг. 2B



Фиг. 3


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

Фиг. 4