(19) Евразийское патентное ведомство

(11) 042505 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2023.02.21

(21) Номер заявки
202190438

(22) Дата подачи заявки
2019.07.15

(51) Int. Cl. *H04L 9/32* (2006.01)

(54) ЗАЩИТА ЦИФРОВОГО ФАЙЛА ОТ ПОДДЕЛКИ

(31) **18187473.6**
(32) **2018.08.06**
(33) **EP**
(43) **2021.06.30**
(86) **PCT/EP2019/068986**
(87) **WO 2020/030382 2020.02.13**

(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-A1-3031169
EP-A2-1770656
US-A1-2009180698
EP-A2-1039420
US-A1-2018219683

(57) Изобретение относится к защите оригинального цифрового файла от подделки и фальсификации связанных с ним данных и, в частности, данных, относящихся к его принадлежности к конкретному пакету оригинальных цифровых файлов, при этом обеспечивая автономную проверку или проверку в режиме "онлайн" аутентичности защищенного цифрового файла и соответствия связанных с ним данных относительно данных подлинного оригинального цифрового файла. Изобретение, в частности, используется для защиты готовых к печати цифровых файлов.

042505 B1

042505 B1

Область техники, к которой относится изобретение

Изобретение относится к области защиты цифровых данных от подделки или фальсификации, а также возможности отслеживания цифровых файлов.

Уровень техники

Проблемы подделки и фальсификации цифровых файлов являются хорошо известными и серьезными, и их количество постоянно растет. Хорошо известным является пример фальсификации данных, нанесенных на оригинальный цифровой документ, такой как цифровой документ, удостоверяющий личность, или цифровая версия диплома, и дело обстоит еще хуже, если рассматривать цифровую копию оригинального (возможно, подлинного) цифрового документа. Простое отслеживание идентификаторов, таких как серийные номера, или даже включение некоторых цифровых водяных знаков, как правило, является слабым решением, поскольку фальсификаторы могут легко скопировать такие номера или цифровые водяные знаки.

Другим недостатком большинства традиционных методов обеспечения аутентичности цифровых файлов или защиты их цифровых данных является то, что они склонны просматривать файлы изолированно, даже если они являются членами четко определенной группы, например, пакета цифровых документов. Это игнорирует ценную аутентификационную информацию.

Таким образом, целью настоящего изобретения является защита печатаемого цифрового файла от подделки и фальсификации связанных с ним данных и, в частности, данных, относящихся к его принадлежности к определенному пакету цифровых файлов. Также целью настоящего изобретения является обеспечение возможности автономной проверки аутентичности печатаемого цифрового файла, защищенного согласно настоящему изобретению, и соответствия содержимого его цифровых данных содержимому подлинного цифрового файла. Настоящее изобретение также направлено на защиту печатаемых цифровых файлов, так что легко проверить аутентичность содержимого данных как печатаемых цифровых файлов, так и их напечатанных версий. В частности, целью настоящего изобретения является защита готовых к печати цифровых файлов, при этом готовый к печати цифровой файл известен как файл печати, который соответствует следующим критериям: все (возможные) изображения RGB преобразуются в цвет CMYK, файл находится в надлежащем формате, таком как PSD, EPS, AL, JPG с высоким разрешением, PDF или TIF, и конечное изображение имеет достаточное разрешение (то есть 300 dpi или выше).

Краткое описание изобретения

Согласно одному аспекту настоящее изобретение относится к способу защиты заданного оригинального цифрового файла, принадлежащего к пакету множества оригинальных цифровых файлов, от подделки или фальсификации, при этом каждый оригинальный цифровой файл включает свои собственные цифровые данные, при этом способ характеризуется тем, что он включает этапы

для каждого оригинального цифрового файла пакета, вычисления посредством односторонней функции связанной с цифровым файлом подписи его цифровых данных;

формирования дерева на основании множества вычисленных подписей цифровых файлов для оригинальных цифровых файлов пакета, содержащего узлы, расположенные согласно заданной упорядоченности узлов в дереве, при этом указанное дерево содержит уровни узлов, начиная от листовых узлов, соответствующих множеству подписей цифровых файлов, соответственно, связанных с множеством оригинальных цифровых файлов в пакете, 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 корневой контрольной цифровой подписи, то есть цифровой подписи посредством односторонней функции конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

связывания с заданным оригинальным цифровым файлом соответствующего цифрового 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 подписи заданного оригинального цифрового файла, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский уровень в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне;

предоставления в распоряжение пользователя контрольной корневой цифровой подписи дерева и

включения в заданный оригинальный цифровой файл соответствующей цифровой защитной маркировки, содержащей машиночитаемое представление его цифровых данных и его соответствующего цифрового ключа верификации,

тем самым получая маркированный оригинальный цифровой файл, цифровые данные которого защищены от подделки или фальсификации.

Таким образом, если цифровая защитная маркировка, включенная в цифровой файл, пригодна к печати в виде штрих-кода, напечатанный документ (включающий напечатанный штрих-код), получаемый путем печати защищенного цифрового файла (посредством обычного печатающего устройства), также защищен, то есть его напечатанные данные 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, контрольная корневая цифровая подпись становится неизменной.

Таким образом, согласно настоящему изобретению переплетение цифровых подписей всех оригинальных цифровых файлов пакета, благодаря структуре дерева и использованию надежных односторонних функций для вычисления значений узлов дерева, вместе с корневой цифровой подписью дерева, сделанной неизменной, и включение цифровых данных и связанного с ним цифрового ключа верификации в цифровой защитной маркировке, включенной в соответствующий оригинальный цифровой файл, позволяют отслеживать и контролировать маркированные файлы и их копии, а также их напечатанные версии, с очень высоким уровнем надежности, при этом предотвращая фальсификацию данных и подделку маркированных файлов.

Маркированный оригинальный цифровой файл может дополнительно содержать данные по доступу к корневому узлу, включенные в него и содержащие информацию, достаточную для обеспечения доступа пользователю к контрольной корневой цифровой подписи корневого узла дерева, соответствующего пакету оригинальных цифровых файлов, при этом указанная информация является ссылкой на интерфейс доступа, выполненный с возможностью приема от пользователя корневого запроса, содержащего цифровые данные или подпись цифрового файла, получаемые из цифровой защитной маркировки маркированного оригинального цифрового файла, и отправки обратно контрольной корневой цифровой подписи соответствующего дерева, при этом интерфейс доступа обеспечивает доступ к, соответственно, 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

виртуальный цифровой файл считается принадлежащим к пакету оригинальных цифровых файлов, при этом указанный виртуальный цифровой файл включает его собственные виртуальные цифровые данные и связанную с виртуальным цифровым файлом подпись, получаемую посредством односторонней функции виртуальных цифровых данных, при этом указанный виртуальный цифровой файл не является реальным, а используется только для генерирования связанной с виртуальным цифровым файлом подписи из его виртуальных цифровых данных; и

контрольная корневая цифровая подпись, связанная с указанным пакетом оригинальных цифровых файлов, вычислена из дерева, имеющего все подписи оригинальных цифровых файлов пакета, включающие подпись виртуального цифрового файла, в виде листовых узлов.

С целью получения более коротких подписей, односторонняя функция может представлять собой хеш-функцию, а цифровая подпись оригинального цифрового файла может представлять собой последовательность заданного множества битов с меньшими значениями разряда, выбранных из битов хеш-значения соответствующих цифровых данных.

В вышеуказанном способе дополнительные цифровые данные, соответствующие цифровым данным, связанным с маркированным оригинальным цифровым файлом, 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 или подпись цифрового файла, получаемые из цифровой защитной маркировки маркированного оригинального цифрового файла, и отправки обратно соответствующих дополнительных цифровых данных.

Цифровые данные маркированного оригинального цифрового файла могут дополнительно включать контрольные характеристические цифровые данные соответствующей уникальной физической характеристики связанного объекта или человека. Более того, уникальная физическая характеристика связанного объекта или человека может представлять собой, соответственно, характеристику защитной маркировки на основе материала, нанесенной на связанный объект или идентифицирующий биометрический признак связанного человека.

В вышеуказанном способе последовательность цифровых подписей в цифровом ключе верификации, включенном в цифровую защитную маркировку, может быть расположена согласно упорядоченности последовательностей узлов, которая отличается от упорядоченности соответствующих узлов, определенных упорядоченностью конкатенации дерева, и цифровая защитная маркировка может дополнительно включать код упорядоченности, связанный с указанной упорядоченностью последовательностей. Эти признаки повышают уровень безопасности в отношении криптоаналитических атак.

Согласно настоящему изобретению в случае распределения цифровых данных соответственных оригинальных цифровых фалов пакета между заданными полями, общими для всех цифровых файлов

пакета, конкретные цифровые данные, относящиеся к этим полям, могут не быть включены в цифровые данные, но могут быть сгруппированы в отдельный блок данных полей, связанный с пакетом, при этом:

i) подпись оригинального цифрового файла вычисляют с помощью односторонней функции конкатенации соответствующих цифровых данных и 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 цифрового файла, защищенного согласно вышеуказанному способу защиты, или соответствия копии такого защищенного цифрового файла относительно оригинального файла, при этом способ включает этапы, при обработке тестового файла, представляющего собой указанный цифровой файл или указанную копию цифрового файла, посредством блока обработки, подключенного к памяти

сохранения в памяти тестового файла;

считывания представления цифровых данных и цифрового ключа верификации на цифровой защитной маркировке сохраненного тестового файла и извлечения, соответственно, соответствующих тестовых цифровых данных и тестового цифрового ключа верификации из указанного считанного представления;

сохранения в памяти контрольной корневой цифровой подписи корневого узла дерева пакета оригинальных цифровых файлов 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 и связанного тестового цифрового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления этапов:

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

извлечения из последовательности цифровых подписей в тестовом цифровом 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 цифровом 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, цифровые данные тестового файла являются данными подлинного цифрового файла.

Если маркированный оригинальный цифровой файл защищен, при этом имея вышеупомянутый отдельный блок данных полей, память блока обработки может дополнительно сохранять связанный блок данных полей, и этап вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем цифровой защитной маркировке на тестовом файле, может включать вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных и сохраненного блока данных полей.

Если цифровой файл был защищен путем сохранения контрольной корневой цифровой подписи в доступной для поиска корневой базе данных, открытой для пользователя, как упомянуто выше, и блок обработки дополнительно подключен к блоку связи, выполненному 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 памяти.

Если защищенный цифровой файл содержит данные по доступу к корневому узлу, как раскрыто выше, и блок обработки дополнительно подключен к блоку связи, выполненному с возможностью от-

правки и приема данных посредством канала связи, вышеуказанный способ верификации может включать предварительные этапы

считывания данных по доступу к корневому узлу, включенных в тестовый файл;

отправки блоком связи посредством канала связи корневого запроса в указанный интерфейс доступа, содержащего цифровые данные или цифровую подпись указанных цифровых данных, получаемых из цифровой защитной маркировки на тестовом файле, и приема обратно соответствующей контрольной корневой цифровой подписи связанного пакета; и

сохранения контрольной корневой цифровой подписи в памяти.

Если маркированный цифровой файл имеет связанные 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 цифровые данные или подпись цифрового файла, получаемые из цифровой защитной маркировки тестового файла, и приема обратно соответствующих дополнительных цифровых данных.

Если защищенный цифровой файл включает контрольные характеристические цифровые данные, как упомянуто выше, и устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики соответственно 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 связанного объекта или человека, способ верификации 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, подлинному объекту или человеку, действительно связанному с подлинным цифровым файлом.

Другой аспект настоящего изобретения относится к цифровому файлу, принадлежащему к пакету множества оригинальных цифровых файлов и защищенному согласно вышеупомянутому способу защиты, при этом каждый оригинальный цифровой файл пакета имеет свои собственные цифровые данные и соответствующий цифровой ключ верификации, указанный пакет имеет соответствующую контрольную корневую цифровую подпись, цифровой файл содержит машиночитаемую защитную маркировку, включающую представление его цифровых данных и его ключа верификации. Цифровые данные цифрового файла могут дополнительно включать контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека. Более того, уникальная физическая характеристика связанного объекта может представлять собой характеристику защитной маркировки на основе материала, нанесенной на связанный объект.

Другой аспект настоящего изобретения относится к системе верификации аутентичности цифрового файла или соответствия копии такого цифрового файла относительно маркированного оригинального цифрового файла, принадлежащего к пакету оригинальных цифровых файлов, 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 пакету оригинальных цифровых файлов, и одностороннюю функцию для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов дерева и упорядоченности конкатенации дерева, запрограммированную в блоке обработки, при этом указанная система выполнена с возможностью

сохранения в памяти тестового файла, представляющего собой указанный цифровой файл или указанную копию цифрового файла;

считывания представления цифровых данных и цифрового ключа верификации на цифровой защитной маркировке сохраненного тестового файла и извлечения, соответственно, соответствующих тестовых цифровых данных и тестового цифрового ключа верификации из указанного считанного представления;

верификации действительного соответствия извлеченных тестовых цифровых данных и тестового цифрового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления на блоке обработки запрограммированных операций:

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

вому узлу в тестовом дереве, соответствующем цифровой защитной маркировке тестового файла;

извлечения из последовательности цифровых подписей в тестовом цифровом 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 цифровом 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 цифровые данные тестового файла являются данными подлинного цифрового файла.

В вышеуказанной системе, если маркированный оригинальный цифровой файл имеет связанный блок данных полей, как упомянуто выше, память блока обработки дополнительно сохраняет связанный блок данных полей, запрограммированные операции вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем цифровой защитной маркировке тестового файла, затем включают вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных и сохраненного блока данных полей.

Если маркированный оригинальный цифровой файл принадлежит к пакету оригинальных цифровых файлов, защищенных путем включения контрольных характеристических цифровых данных соответствующей уникальной физической характеристике связанного объекта или человека, как упомянуто выше, вышеуказанная система дополнительно оснащена датчиком, подключенным к блоку обработки и выполненным с возможностью обнаружения уникальной физической характеристики связанного объекта или человека, и при этом блок обработки запрограммирован для извлечения соответствующих характеристических цифровых данных из сигнала обнаружения, принятого от датчика, система сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике связанного объекта или человека, при этом система может дополнительно быть выполнена с возможностью

обнаружения с помощью датчика уникальной физической характеристики субъекта, представляющего собой указанный связанный объект или человека, 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, при условии заданного критерия допустимого отклонения, доставки указания того, что субъект считается подлинным.

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 пакета оригинальных цифровых файлов согласно настоящему изобретению.

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

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

На фиг. 3 проиллюстрирован пакет цифровых документов, относящихся к компонентам самолета, 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 пакета цифровых файлов, и к способу вычисления кодирования верифицированной информации, которая может быть связана с каждым цифровым файлом. На фиг. 1 проиллюстрирована группа или "пакет" цифровых файлов $A_1...,A_8$, содержащие цифровое представление машиночитаемой защитной маркировки 110 (в данном случае проиллюстрированной двухмерным штрих-кодом). В дальнейшем, выражение "цифровая защитная маркировка 110" фактически означает "цифровое представление машиночитаемой защитной маркировки 110". На фиг. 1 фактически проиллюстрирована группа или "пакет" цифровых файлов и связанное с ними дерево, при этом для упрощения показаны только восемь оригинальных цифровых файлов: $A_1...,A_8$. Также для упрощения, дерево, связанное с пакетом файлов $A_1...,A_8$, в данном случае представляет собой простое двоичное дерево. Цифровой файл может относиться к промышленному товару или его упаковке, физическому документу или изображению, упаковке, содержащей несколько товаров (например, блистерной упаковке с лекарством), или контейнеру, содержащему поддоны с картонными коробками с товарами и т.д. Не только объект, но даже человек может быть "связан" с цифровым файлом в контексте вариантов осуществления настоящего изобретения; например, авторизованные участники мероприятия или члены группы, или члены стада или стаи могут нести какую-либо форму идентификационного значка или иметь физическую маркировку, содержащую данные, записанные в соответствующем цифровом файле.

Пакет цифровых файлов 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 может быть определен цифровой файл A_i (имеющий цифровое содержимое D_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 пакету из восьми изделий, и обработано как любое из других семи реальных изделий, 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 $A_1,A_2,...,A_7,A_8$ пакета (где возможно $A_8 \equiv A_v$) соответственные цифровые данные изделия $D_1,D_2,...,D_7,D_8$ (где возможно $D_8 \equiv D_v$) 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 связанном изделии (например, напечатанных на изделии или на этикетке, прикрепленной к изделию) посредством считывателя, выполненного с возможностью создания соответствующих цифровых данных цифрового файла A_i. Дополнительные цифровые данные (например, команда для использования связанного изделия или команды безопасности и т.д.) могут быть связаны с извлеченными данными для создания цифровых данных изделия D_i.

Для виртуального изделия A_v связанные цифровые данные могут включать, например, идентификационный номер пакета, количество изделий в пакете, (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 пакета его соответственные цифровые данные изделия $D_1,D_2,...,D_7,D_8$ предпочтительно преобразовываются математическим путем, так что они по существу скрыты, хотя это не является абсолютным требованием для любого варианта осуществления. Это преобразование, применяемое к цифровым данным D_i изделия A_i, служит для создания соответствующей цифровой подписи x_i. Эту цифровую подпись получают посредством односторонней функции, то есть функции, которую легко вычислить, но трудно инвертировать (см. S. Goldwasser and M. Bellare "Lecture Notes on Cryptography", MIT, июль 2008 г., http://www-cse.ucsd.edu/users/mihir).

Одним из таких выгодных преобразований является, например, применение хеш-функции H( ) = hash( ) к цифровым данным, 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 цифрового файла (например, связанного с изделием) независимо от размера цифровых данных и размера пакета соответствующих цифровых файлов. Хеш-функция - это хорошо известный пример односторонней функции. Если используется криптографическая хеш-функция, такая как класс функций SHA (Secure Hash Algorithm), например SHA-256, то существуют дополнительные преимущества, заключающиеся в том, что функция практически необратима и устойчива к коллизиям, то есть вероятность того, что две разные группы входных данных приведут к одним и тем же выходным данным, ничтожна. Как будет понятно из приведенного ниже описания, это также не является требованием настоящего изобретения, хотя оно выгодно по тем же причинам, что и в других приложениях. Как показано на фиг. 1, значения $x_1,x_2,x_3,...,x_8$ представляют собой хеш-значения, то есть связанные с изделиями цифровые подписи соответственных наборов данных изделий, а именно $x_j = H(D_j)$, для j = 1,...,8 (в случае $A_8 = A_v$, то $D_8 = D_v$ 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 показан пакет 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 их соответственных связанных с изделием цифровых данных $D_1,...D_8$ (символически представлено на файлах A_i на фиг. 1 посредством последовательности битов "0" и "1") посредством дерева цифровых подписей цифровых данных. 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, то есть "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, то есть 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, то есть 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 (то есть 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)), то есть $a(2,1) = H(H(D_1)+ H(H(D_2))$, (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 конкатенации, задействованных в дереве, практически невозможно получить корне-

вое значение, если какой-либо бит цифровых данных изменяется в узле (в частности, в листовом узле). Более того, если в пакет 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 пакета.

Согласно настоящему изобретению контрольная корневая цифровая подпись R пакета оригинальных цифровых файлов 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 оригинального цифрового файла A_i пакета соответствующий цифровой ключ верификации 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 оригинального цифрового файла A_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. В примере фиг. 1 представлены восемь ключей верификации $k_1,...,k_8$, соответственно, соответствующих восьми изделиям $A_1,...,A_8$ пакета 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 $a(1,1) = x_1$ листового узла $a(1,2) = x_2$ в k_1 (a(1,2) представляет собой другой листовой узел, имеющий такой же родительский узел, то есть узел a(2,1), что и листовой узел, соответствующий цифровой подписи изделия x_1, то есть узел a(1,1)), получают значение родительского узла a(2,1) посредством $a(2,1) = H(a(1,1)+a(1,2))$ (то есть $a(2,1) = H(x_1 + x_2)$),

ii) из полученного a(2,1) и значения следующего узла в k_1, то есть a(2,2) следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, то есть узел a(3,1), что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, то есть 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, то есть a(3,2) предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, то есть корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, то есть 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, то есть узел a(2,1), что и листовой узел, соответствующий цифровой подписи изделия x_2, то есть 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, то есть a(2,2) следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, то есть узел a(3,1), что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, то есть 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, то есть a(3,2) предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, то есть корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, то есть 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, то есть узел a(2,2), что и листовой узел, соответствующий цифровой подписи изделия x_3, то есть 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, то есть a(2,1) следующего уровня узлов, отличных от листовых, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, то есть узел a(3,1), что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, то есть 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, то есть a(3,2) предпоследнего уровня узлов, который представляет собой узел, отличный от листового, имеющий такой же родительский узел в дереве, то есть корневой узел, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне, то есть 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 уровня в k_4, то есть 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, то есть 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, то есть 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, то есть 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, то есть 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, то есть 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, то есть 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, то есть 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, то есть 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, то есть 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 (то есть 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 (то есть 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 цифровая защитная маркировка 110 цифрового файла A_i пакета изделий включает информацию о верификации V_i, что обеспечивает операции как проверки в режиме "онлайн", так и автономной проверки аутентичности маркированного файла, соответствия связанных с ним данных относительно данных подлинного маркированного файла, путем обеспечения уникальной, неизменной и защищенной от подделки связи между цифровыми данными D_i A_i и тем фактом, что маркированный оригинальный цифровой файл A_i принадлежит к указанному пакету 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 пакета или контрольной корневой цифровой подписи R дерева, связанного с пакетом, путем первого считывания цифровых данных D_i и соответствующего цифрового ключа верификации k_i на машиночитаемой защитной маркировке 110 цифрового файла A_i, затем вычисление потенциальной цифровой подписи X_i посредством односторонней функции считанных цифровых данных 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 цифровом 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 цифровую 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 цифровой защитной маркировке согласно настоящему изобретению, является компактным и позволяет использовать обычное представление двухмерных штрих-кодов (например, QR-кода) (в частности используемых для готовых к печати цифровых файлов) 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 цифрового файла и соответствия его данных относительно данных подлинного (оригинального) цифрового файла. 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 (то есть информацию о верификации V), которые должны быть включены в цифровую защитную маркировку, если цифровые данные D_i соответственных оригинальных цифровых файлов A_i пакета распределены между заданными полями, которые являются общими для всех цифровых файлов пакета, цифровые данные, относящиеся к этим полям, не включены в каждые цифровые данные D_i, но сгруппированы в отдельном блоке данных полей FDB, связанном с пакетом цифровых изделий, и

цифровую подпись x_i оригинального цифрового файла A_i пакета затем вычисляют с помощью односторонней функции H конкатенации соответствующих цифровых данных D_i и цифровых данных блока данных полей FDB, то есть $x_i = H(D_i+FDB)$; 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 цифровыми файлами пакета, классифицируются согласно некоторым полям для структурирования данных: наприме,, для фармацевтического продукта, связанного с защищенным цифровым файлом, 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.

Есть много известных методов кодирования информации. Любой такой метод можно использовать в реализациях любого варианта осуществления настоящего изобретения. Одна из распространенных форм маркировки - это хорошо известный QR-код (в виде представления двухмерного изображения, включенного в цифровой файл). Как хорошо известно, для заданной области, чем больше данных может кодировать QR-код, тем выше плотность модуля (грубо говоря, плотность черных/белых "квадратов") и тем большее разрешение требуется для печати и считывания. Помимо плотности (в количестве квадрата модулей), QR-коды также обычно классифицируются в зависимости от того, какой уровень исправления ошибок они включают. В настоящее время четыре разных стандартных "уровня", L, M, Q и H, каждый из которых представляет степень "повреждения", то есть потери данных, изображение QR-кода может выдержать и из которых может восстановиться. Уровни L, M, Q и H могут выдержать приблизительно 7, 15, 25 и 30% повреждения соответственно.

В следующей таблице приведены, по меньшей мере, приблизительные значения для разных версий QR-кода.

Версия	Размер (в модулях)	Количество кодируемых битов	
		уровень L ECC	уровень H ECC
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 цифровой 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, некоторые схемы защиты данных включают подписи, которые растут по мере увеличения количества элементов пакета, и которые могут недопустимо ограничивать размер пакета с точки зрения того, сколько битов может кодировать цифровая 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 оригинальных цифровых файлов пакета для определения цифровых ключей верификации для разных цифровых файлов 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) цифрового(ых) файла(ов) A_v. Также можно было бы осуществлять вычисления хеширования, связанные с файлами, извне (например, на подключенном удаленном сервере), например, где бы ни изготовлялись цифровые файлы, чтобы избежать необходимости передавать необработанные цифровые данные D_i по сети с этого сайта (или сайтов) к системе защиты, если есть проблема. Для каждого цифрового файла A_i компилируется соответствующая информация о верификации V_i, которая кодируется (предоставляется) в некоторой форме машиночитаемой цифровой защитной маркировки 110, которая затем включается в соответственное изделие.

Для любого "виртуального" цифрового файла 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 цифрового файла A_i пакета цифровых файлов, соответствующие цифровые данные D_i и соответствующий цифровой ключ верификации k_i: то есть $V_i = (D_i,k_i)$.

Дополнительные цифровые данные могут дополнительно быть связаны с цифровым файлом и могут включать, например, значение пакета, то есть 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 пакета, информация о дате/времени, название продукта, URL-адрес, который указывает на другую онлайн-информацию, связанную либо с отдельным товаром (например, изображение товара или его этикетки или упаковки и т.д.), либо с пакетом, либо с поставщиком/изготовителем, номер телефона, по которому можно позвонить для верификации и т.д. Дополнительные цифровые данные могут храниться в доступной для поиска информационной базе данных, открытой для пользователя (посредством интерфейса информационной базы данных).

После вычисления цифровой верификации k_i оригинального цифрового файла A_i и включения (то есть посредством кодирования или любого выбранного представления данных) вместе с соответствующими цифровыми данными D_i в машиночитаемую цифровую защитную маркировку 110 в цифровом файле A_i, полученный в результате маркированный оригинальный цифровой файл и связанные с ним цифровые данные действительно защищены от подделки и фальсификации.

Пользователь, получатель цифрового файла, такого как A_1 например, может затем сканировать (или иным образом считывать) с помощью устройства для формирования изображения (считывателя) цифровую защитную маркировку A_1 и извлекать цифровые данные D_1 и цифровой ключ верификации k_1, (и любую другую информацию, которая могла быть закодирована в маркировке). Для верификации маркированного цифрового файла A_1 пользователь должен сначала извлечь информацию о верификации $V_1=(D_1,k_1)$ из цифровой защитной маркировки 110 A_1 и, таким образом, вычислить цифровую подпись x_1 из извлеченных цифровых данных D_1: чтобы выполнить такую операцию, пользователь должен знать

одностороннюю функцию, которая используется для вычисления цифровой подписи, 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 цифровых файлов 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 цифрового файла 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 дополнительно 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 x_1 и значений узлов согласно последовательности узлов, определенных в цифровом ключе верификации k_1, см. выше пункт "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 цифровой защитной маркировке 110 и подтверждает, что цифровой файл A_1 принадлежит правильному пакету.

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

Пользователь, получатель цифрового файла, такого как A_1, например, может затем сканировать (или иным образом считывать) с помощью считывателя цифровую защитную маркировку на A_1 и извлекать цифровые данные D_1 и цифровой ключ верификации k_1 (и любую другую информацию, которая могла быть закодирована в цифровой защитной маркировке). Примером считывателя является компьютер с дисплеем или даже (программируемый) смартфон. Для верификации маркированного файла A_1 пользователь должен сначала извлечь информацию о верификации $V_1=(D_1,k_1)$ из цифровой защитной маркировки на A_1 и, таким образом, вычислить подпись цифрового файла x_1 из извлеченных цифровых данных D_1: чтобы выполнить такую операцию, пользователь должен знать одностороннюю функцию, которая используется для вычисления цифровой подписи, в данном случае это хеш-функция H(), а затем выполнить операцию $x_1=H(D_1)$ для получения полных данных (x_1,k_1), необходимых для вычисления соответствующей потенциальной корневой цифровой подписи B^c.

Пользователь может, например, безопасно принять одностороннюю функцию (например, используя пару открытого и личного ключей) или запросив ее у поставщика цифровых файлов или любого другого объекта, который создал подписи и ключи или уже запрограммировал их в блок обработки считывателя.

Предпочтительно контрольная корневая цифровая подпись (то есть значение пакета) R хранится в доступной для поиска корневой базе данных, к которой может получить доступ (через канал связи) пользователь с помощью своего компьютера, оснащенного блоком связи, как это имеет место с вышеуказанным примером смартфона. Пользователь, которому необходимо верифицировать цифровой файл A_1, может просто отправить корневой запрос со своего смартфона на адрес базы данных через интерфейс доступа к базе данных, запрос, содержащий цифровые данные D_1, считанные на цифровой защитной маркировке 110 A_1 (или вычисленную цифровую подпись $x_1 = H(D_1)$), что позволяет извлечь соответствующее контрольное значение пакета 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, то есть оригинальным цифровым файлом, сохраненным в памяти, и его атрибутами, то есть связанными цифровыми данными и его принадлежностью к конкретному пакету цифровых файлов, практически неизменно посредством соответствующей корневой цифровой подписи.

Вышеупомянутый способ верификации цифрового файла A_i также может служить для аутентификации читаемого человеком содержимого данных A_i на соответствующей печатной версии цифрового файла A_i. Действительно, пользователь может считать на дисплее компьютера соответствующие цифровые данные D_i как декодированные из цифровой защитной маркировки в цифровом файле A_i посредством компьютера и визуально проверить, соответствует ли отображаемая информация напечатанным данным на печатной версии цифрового файла.

В предпочтительном варианте осуществления цифровые данные D_i дополнительно включают характеристические цифровые данные CDD соответствующей уникальной физической характеристики объекта или человека, связанные с маркированным оригинальным цифровым файлом A_i, которые можно использовать для (материальной) аутентификации связанного объекта или связанного человека путем сравнения характеристических цифровых данных, извлеченных из цифровой защитной маркировки, и соответствующих данных обнаружения уникальной физической характеристики, получаемых от подходящего датчика. Таким образом, с помощью характеристических цифровых данных, соответствующих уникальной физической характеристике в цифровом файле 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 характеристических цифровых данных CDD_i, то есть $UPS_i = H(CDD_i)$. 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 объекта OBJ_i, связанного с цифровым файлом A_i, рассмотрим простое цифровое изображение, полученное отображением объекта OBJ_i (или конкретной зоны на OBJ_i), например, посредством камеры смартфона, 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 уникальной физической подписи для A_i. Предпочтительно, UPS_i, то есть контрольные данные уникальной физической подписи для цифрового файла 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 D_i, считываемые на цифровой защитной маркировке в цифровом файле A_i, или их соответствующую подпись цифрового файла x_i). Таким образом, сохраненная UPS_i приобретает неизменный характер. Копия CDD_i может дополнительно храниться в памяти смартфона пользователя (или считывателя, или компьютера). В варианте осуществления копию UPS_i можно также дополнительно хранить в памяти смартфона пользователя (или считывателя, или компьютера) для обеспечения операции автономной проверки.

Проверку аутентичности цифрового файла 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 смартфоне) на цифровой защитной маркировке, включенной в цифровой файл A_i, и сравнения их с контрольными характеристическими цифровыми данными CDD_i, сохраненными в памяти смартфона: в случае совпадения $CDD_i^c = CDD_i$, цифровой файл A_i считается подлинным (его цифровое содержимое соответствует содержимому подлинного маркированного оригинального цифрового файла). Если контрольные характеристические цифровые данные CDD_i не хранятся в памяти смартфона, а напротив, контрольные данные уникальной физической подписи UPS_i хранятся в памяти смартфона (с тем преимуществом, что они занимают гораздо меньше памяти по сравнению с CDD), 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 характеристических цифровых данных CDD_i^c, извлеченных из цифровых данных D_i, то есть $UPS_i^c = H(CDD_i^c)$, совпадают с контрольными данными уникальной физической подписи UPS_i, сохраненными в памяти.

Пользователь может дополнительно проверить аутентичность принятого цифрового файла A_i, все еще посредством автономного процесса (самоконтроль), путем обнаружения указанной уникальной физической характеристики на объекте или человеке, связанной с цифровым файлом A_i, посредством датчика, выполненного с возможностью осуществления такого измерения (в данном случае камеры смартфона), и получения потенциальных характеристических цифровых данных CDD_i^c из обнаруженной характеристики (в данном случае цифрового изображения, снятого смартфоном). Таким образом, пользователь может сравнивать (посредством блока обработки изображения его смартфона, или визуально на дисплее смартфона) полученные CDD_i^c с копией контрольных CDD_i (сохраненных в памяти смартфона): в случае "обоснованного" совпадения $CDD_i^c \approx CDD_i$ (то есть два цифровых данных согласуются с неким

заданным критерием отклонения или схожести), цифровой файл A_i считается подлинным (то есть его цифровое содержимое соответствует содержимому подлинного маркированного оригинального цифрового файла).

Более того, пользователь может также дополнительно вычислить соответствующие потенциальные данные уникальной физической подписи из копии контрольных CDD_i, сохраненных в памяти смартфона в виде $UPS_i^c = H(CDD_i)$, и сравнить их с контрольными данными физической подписи UPS_i, сохраненными в памяти смартфона: в случае совпадения $UPS_i^c = UPS_i$, подтверждается, что цифровой файл A_i является подлинным с более высокой степенью достоверности (поскольку достаточно одного бита разницы, чтобы вызвать несовпадение). Более того, в случае совпадения, также устанавливают аутентичность цифровых данных D_i, связанных с A_i, которые были верифицированы как соответствующие данным подлинного цифрового файла, как раскрыто выше, путем извлечения соответствующего значения пакета R из считанной информации о верификации (D_i,k_i), сохраненной в цифровой защитной маркировке в A_i.

В варианте осуществления проверку аутентичности цифрового файла A_i пользователем можно осуществлять посредством процесса в режиме "онлайн". В данном случае, контрольные данные, то есть характеристические цифровые данные CDDi и/или контрольные данные уникальной физической подписи UPSi, хранятся в доступной для поиска базе данных, открытой для пользователя, где контрольные данные, относящиеся к цифровому файлу A_i, хранятся в связи с, соответственно, соответствующими цифровыми данными D_i (включенными в цифровую защитную маркировку в A_i) или с соответствующей подписью цифрового файла x_i (что можно вычислить пользователем, как только данные Di извлекают из цифровой защитной маркировки посредством операции $x_i=H(D_i)$): контрольные данные можно запросить путем отправки в базу данных запроса, содержащего, соответственно, D_i или x_i.

Обычным способом защиты объекта является нанесение на него защитной маркировки на основе материала (возможно, защищенной от несанкционированного доступа), то есть маркировки, обладающей обнаруживаемым внутренним физическим или химическим свойством, которое очень трудно (если не невозможно) воспроизвести. Если пригодный датчик обнаруживает это внутреннее свойство маркировки, данная маркировка считается подлинной с высокой степенью достоверности, а следовательно, и соответствующий маркированный объект. 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 объекте, 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 объекта, 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 объекте, которые при просмотре с достаточным увеличением также могут привести к уникальной подписи и т.д. Основная проблема, связанная с внутренним свойством отпечатка пальца объекта, это его устойчивость к старению или износу. Однако защитная маркировка на основе материала не всегда позволяет также защитить данные, связанные с маркированным объектом: 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 объекта невозможна. Согласно настоящему изобретению объект, маркированный защитной маркировкой на основе материала и связанный с (цифровым образом) маркированным цифровым файлом, защищен переплетением, полученным в результате факта того, что характеристические цифровые данные, соответствующие уникальной физической характеристике маркированного объекта, или их соответствующие данные уникальной физической подписи, являются неизменными (благодаря публикации или хранению агрегированной цифровой подписи в блокчейне) и защищены от подделки, связаны с цифровыми данными в цифровой защитной маркировке, представляющей собой часть связанного цифрового файла. Таким образом, настоящее изобретение можно использовать для защиты как пакета объектов, так и соответствующего пакета связанных цифровых файлов.

Конечно, любое другое известное внутреннее физическое/химическое свойство можно использовать для получения характеристических цифровых данных CDD_i, относящихся к уникальной физической характеристике объекта OBJ_i, связанной с цифровым файлом A_i и соответствующими данными уникальной физической подписи UPS_i. В качестве другого иллюстративного примера можно напечатать двухмерный штрих-код, образующий защитную маркировку на основе материала, на объекте 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 т, которое служит "отпечатком пальца" материала краски. Достаточно осветить штрих-код возбуждающим светом в окне длины волны освещения, охватывающем окно длины волны возбуждения пигмента, и собрать полученный в результате люминесцентный свет со штрих-кода с помощью датчика, выполненного с возможностью определения интенсивности света в пределах окна длины волны люминесцентного испускания, чтобы аутентифицировать штрих-код, а значит, и объект. Например, считыватель пользователя может быть оснащен вспышкой, выполненной с возможностью подачи возбуждающего света на штрих-код, фотодиодом, выполненным с возможностью сбора соответствующего профиля интенсивности люминесцентного света I(t)(в течение интервала времени обнаружения) со штрих-кода, и ЦП считывателя, 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 объекта 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, объект считаются подлинными, если $\tau_c \approx \tau$ (в заданном диапазоне отклонения). В данном случае характеристические цифровые данные CDD_i маркированного объекта OBJ_i включают, по меньшей мере, контрольное значение τ времени затухания (и, возможно, данные, относящиеся к окну длины волны возбуждения и окну длины волны испускания). Как видно из приведенных выше примеров, технический результат включения контрольных (уникальных) характеристических цифровых данных в информацию о верификации цифровой защитной маркировки связанного цифрового файла A_i заключается в обеспечении защищенной от подделки связи между цифровыми данными цифрового файла и данными аутентификации связанного с ним объекта.

Другой иллюстративный вариант осуществления настоящего изобретения относится к пакету биометрических идентификационных документов, например, биометрические цифровые паспорта, как показано на фиг. 2А. Каждый цифровой паспорт, как цифровой файл, связан с соответствующим человеком, то есть с владельцем паспорта. Для ясности цифровые данные A_1 представлены на фиг. 2А в виде эквивалентной текстовой и буквенно-цифровой информации (то есть читаемой человеком), например, как она может быть отображена из цифрового файла pdf ("Portable Document Format"), а цифровая защитная маркировка показана в виде эквивалентного обычного двухмерного рисунка QR-кода. Этот вариант осуществления настоящего изобретения особенно полезен для создания печатаемых цифровых файлов, таких как готовые к печати цифровые файлы, чтобы позволить печатающему устройству доставлять напечатанный защищенный документ непосредственно из соответствующего защищенного печатаемого цифрового файла (например, цифрового файла, относящегося к документу, удостоверяющему личность, диплому, договору и т.д.).

В этом примере по-прежнему используют хеш-функцию как одностороннюю функцию для подписывания цифровых данных паспорта, предпочтительно хеш-функцию SHA-256 ввиду ее хорошо известной надежности. Действительно, с учетом заданного размера пакета, хэш-функция, которая выбрана (имеющая известный список сегментов) для подписания цифровых данных паспорта, является, таким образом, примером односторонней функции шифрования, так что каждый отдельный цифровой паспорт имеет отдельную цифровую подпись паспорта, что делает подпись уникальной. Домен хеш-функции (то есть набор возможных ключей) больше, чем ее диапазон (то есть количество различных индексов таблицы), он будет отображать несколько разных ключей в один и тот же индекс, что может привести к конфликтам: таких конфликтов можно избежать, когда размер пакета 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. 2А показан пример цифрового биометрического паспорта A_1, защищенного машиночитаемой цифровой защитной маркировкой 210 (в данном случае QR-кодом), кодированной в A_1, и содержащего цифровые данные 230 паспорта, содержащие обычные данные паспорта, например, цифровые данные, представляющие собой название документа 230a ("Паспорт"), набор биографических данных владельца паспорта 230b: фамилия ("Доу"), имя ("Джон"), пол ("М"), дата рождения ("20 марта 1975 г."), гражданство ("США"), место проживания ("Де-Мойн"), место рождения ("Окленд"), дата 230c выдачи ("24 февраля 2018 г.") и дата окончания срока действия 230d ("23 февраля 2020 г."). Эти цифровые данные паспорта могут дополнительно содержать некоторый(е) (уникальный(е)) серийный(е) номер(а) 235,

присвоенный органом, выдающим паспорт (в данном случае "12345"). Цифровые данные паспорта дополнительно содержат биометрические данные владельца паспорта в виде характеристических цифровых данных (CDD), соответствующих уникальной физической характеристике человека, связанного с цифровым паспортом. Машиночитаемое представление 230e (например, буквенно-цифровое) данных, характеризующих указанную уникальную физическую характеристику (не показана), соответствующую указанным биометрическим данным, связано с цифровыми данными 230 паспорта. Представление цифровых данных следует понимать в широком смысле этого термина: для этого представления данных необходимо только обеспечение извлечения оригинальных цифровых данных. Машиночитаемое представление 230e данных, то есть биометрические данные, уникальной физической характеристики, может соответствовать, например, идентификационным данным отпечатка пальца или идентификационным данным радужной оболочки глаза владельца цифрового 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 цифрового паспорта A_j из пакета μ доставленных цифровых биометрических паспортов, в данном случае где $\mu = 1024$, связанные с паспортом цифровые данные D_j включают вышеупомянутые цифровые данные 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, то есть "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, Di 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 цифровыми 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 качестве данных 240 по доступу к информации в цифровой паспорт: в данном случае эти данные по доступу к информации закодированы в цифровом представлении QR-кода, содержащего 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 паспорта с помощью односторонней хэш-функции цифровых данных паспорта D_j, соответствующих цифровым данным 230a-230e цифрового 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 цифровых паспортов в пакете для всех различных владельцев.

Для всех подписей паспортов в пакете контрольную корневую цифровую подпись R вычисляют согласно упорядоченности дерева и упорядоченности конкатенации дерева связанного (двоичного) дерева, как раскрыто выше. Поскольку в пакете $\mu = 1024$ 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., 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 цифровой ключ верификации k_j представляет собой последовательность из 10 значений узлов. Цифровая защитная маркировка 210 цифрового паспорта A_j включает цифровые данные паспорта D_j и соответствующий цифровой ключ верификации k_j (то есть информацию о верификации $V_j = (D_j,k_j)$).

Для операции проверки действительного соответствия цифровых данных паспорта D_j и цифрового ключа верификации k_j в цифровой защитной маркировке 210 биометрического цифрового паспорта A_j данным подлинного биометрического цифрового паспорта, принадлежащего к пакету μ биометрических цифровых паспортов, имеющему значение пакета R, необходимо только вычисление цифровой подписи паспорта $x_j = H(D_j)$ и верификация того, что x_j и цифровой 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 цифровой 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 цифрового 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. Цифровая защитная маркировка 210 паспорта 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) цифрового 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 пакета 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 пакетов биометрических цифровых паспортов. В примере, показанном на фиг. 2B, информационная база 250 данных является локальной (то есть непосредственно доступна органам, без необходимости использования общедоступной сети связи). Кроме того, эти органы оснащены сканерами 270 отпечатков пальцев для захвата отпечатков пальцев людей и вычисления соответствующих машиночитаемых представлений данных, характеризующих снятые отпечатки пальцев, то есть биометрические данные 230e.

Во время проверки личности Джона Доу, скажем, сотрудником полиции или таможни, сотрудник принимает защищенный биометрический цифровой паспорт A_1 Джона Доу, считывает и декодирует информацию о верификации (D_1,k_1), сохраненную в цифровой защитной маркировке 210 цифрового паспорта, посредством пригодного считывателя, который может представлять собой, например, подходящим образом запрограммированный компьютер 290, при этом компьютер подключен к локальным хранилищам 250. После считывания цифровых данных паспорта D_1 и цифрового 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 пакета 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)),

то есть 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" (то есть 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 (то есть 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 цифровой защитной маркировке 210 с помощью компьютера 290 и сканирует отпечаток пальца человека с помощью сканера 270 отпечатков пальцев, подключенного к компьютеру 290, и получает биометрические данные соответствующего человека: сотрудник затем проверяет посредством программы, запущенной на компьютере 290, сходны ли извлеченные биометрические данные 230e (в пределах заданной погрешности) с полученными биометрическими данными человека.

Если два лица и биометрические данные считаются 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. Таким образом, с помощью защищенного биометрического цифрового паспорта согласно настоящему изобретению простая автономная проверка может быстро обнаружить любое мошенничество.

Фактически, можно даже уменьшить цифровой биометрический паспортный документ до простого цифрового файла с простым цифровым представлением двухмерного штрих-кода (как в вышеупомянутом примере QR-кода), включающего информацию о верификации V=(D,k): с V, содержащим биографические данные владельца и (уникальные) биометрические данные, такие как отпечаток пальца владельца (в цифровых данных D паспорта) и ключ верификации. В действительности, согласно настоящему изобретению даже этот "уменьшенный" защищенный цифровой 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 (возможно, цифровой) 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 (цифровые) технические паспорта его соответственных компонентов. Тем не менее, поддельные компоненты могут иметь соответствующий поддельный цифровой технический паспорт, и поэтому не очевидно (если только, например, не проводить технические испытания) выявить мошенничество. Например, как быть уверенным, что цифровой 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 пакету "компонентов" (или "объектов") для этого конкретного самолета.

В конкретном иллюстративном варианте осуществления, показанном на фиг. 3, каждый компонент пакета самолета, то есть каждый разрешенный компонент самолета для установки или ремонта на данном самолете, имеет соответствующий цифровой идентификационный документ компонента самолета AC-ID, который содержит такие же цифровые данные компонента, как в обычном техническом паспорте (например, идентификационный код самолета, название изготовителя самолета, техническое название компонента, уникальный серийный номер компонента, название изготовителя компонента и дата изготовления компонента) вместе с дополнительными цифровыми данными, соответствующими идентификационному коду самолета, названию изготовителя самолета, дате сборки компонента на самолете, имени специалиста, ответственного за выполнение проверки соответствия, вместе с датой проверки соответствия и соответствующей (уникальной) цифровой подписью проверяющего. Кроме того, каждый цифровой идентификационный документ AC-ID компонента самолета защищен посредством добавленной к нему машиночитаемой цифровой защитной маркировки. Для ясности цифровые данные AC-ID:A_{125} представлены на фиг. 3 в виде эквивалентной текстовой и буквенно-цифровой информации (то есть читаемой человеком), а цифровая защитная маркировка 310 показана в виде эквивалентного обычного двухмерного рисунка QR-кода.

Предпочтительно, каждый раз при замене компонента или набора компонентов на самолете создаются соответствующие защищенные цифровые документы AC-ID, а также создается соответствующая обновленная версия пакета 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 соответствующему пакету

установленных компонентов (в данном случае всего μ компонентов) и задокументированы в соответствующем пакете связанных μ цифровых файлов, то есть цифровом идентификационном документе AC-ID. Цифровая защитная маркировка 310 (в данном случае в виде QR-кода) включена в каждый цифровой идентификационный документ компонента самолета, например, AC-ID:A_{125}, который связан с соответствующим компонентом самолета, в данном случае A_{125}, установленном на самолете HB-SNO. На фиг. 3, в частности, показан компонент A_{125} пакета самолета, представляющий собой лопатку турбины, адаптированную к типу реактора, установленную на самолете HB-SNO и маркированную уникальным заводским серийным номером (в данном случае 12781, обычно выгравированным изготовителем). Цифровые данные компонента D_{125} в цифровой защитной маркировке 310 цифрового идентификационного документа компонента самолета AC-ID:A_{125}, связанного с компонентом A_{125}, содержат цифровые данные, соответствующие данным технического паспорта: идентификационный код 330a самолета (в данном случае HB-SNO), название 330b изготовителя самолета (в данном случае AerABC), техническое название 330c компонента (в данном случае лопатка турбины - 1-е 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} цифрового файла AC-ID:A_{125} компонента A_{125} вычисляют посредством односторонней хеш-функции H в виде $x_{125} = H(D_{125})$. Таким же образом, все цифровые подписи компонента x_i цифровых данных D_i компонента A_i вычисляют посредством односторонней хеш-функции H в виде $x_i = H(D_i)$(в данном случае i = 1,...,μ).

Согласно настоящему изобретению дерево, связанное с пакетом компонентов $A_1,...,A_\mu$ (в данном случае двоичное дерево), и, таким образом, с соответствующим пакетом цифровых файлов AC-ID:A_1,...,AC-ID:A_μ, построено с μ листовых узлов a(1,1),...,a(1,μ), соответственно, соответствующих μ цифровых подписей компонентов $x_1,...,x_\mu$ соответственных цифровых данных компонента $D_1,...,D_\mu$ цифровых идентификационных документов AC-ID:A_1,...,AC-ID:A_μ компонентов $A_1,...,A_\mu$. В данном случае упорядоченность узлов двоичного дерева является обычной упорядоченностью, то есть 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 пакета μ компонентов самолета $A_1,...A_\mu$ 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, то есть 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 пакета цифровой ключ верификации k_i, соответствующий цифровой подписи компонента x_i (то есть 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 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 с компонентом цифровые данные D_i и соответствующий цифровой ключ верификации k_i встроены в цифровую защитную маркировку 310, включенную в соответствующий цифровой 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 цифровом файле AC-ID:A_{125} компонента A_{125}, подлежащего контролю, или его цифровой

ключ верификации k_{125}, считываемый на цифровой защитной маркировке 310 на соответствующем документе AC-ID:A_{125} с помощью пригодного считывателя, как, например, компьютера, запрограммированного для декодирования содержимого цифровой защитной маркировки, и примет обратно соответствующее значение пакета B. В предпочтительном варианте, обеспечивающем полную автономную проверку, компьютер специалиста имеет 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 цифровой защитной маркировке 310 AC-ID:A_{125}, проверки совпадения уникального серийного номера 330d (в данном случае 12781), извлеченного из D_{125}, с серийным номером, физически нанесенным на установленный компонент самолета A_{125}, вычисления соответствующей цифровой подписи компонента x_{125} (например, путем запуска запрограммированного приложения на ЦП блока обработки компьютера, который вычисляет подпись $x_{125} = H(D_{125})$ из считанных цифровых данных D_{125}), вычисления потенциального значения пакета R^c посредством односторонней функции H, запрограммированной на ЦП компьютера в виде хеш-значения конкатенации значения листового узла $a(1,125)=x_{125}$ и значений узлов, заданных в соответствующем цифровом ключе верификации k_{125}, и проверки совпадения потенциального значения пакета R^c со значением контрольных корневых цифровых подписей, сохраненных в памяти компьютера (то есть контрольное значение R, соответствующее самолету HB-SNO). В случае полного совпадения (то есть совпадения серийных номеров и $R^c = R$), компонент A_{125} считается подлинным и принадлежит к (обновленному) пакету 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 правильному пакету для данного самолета), и должен быть заменен.

Таким же образом, настоящее изобретение позволит обнаруживать мошенничество (или ошибки) в пакетах защищенных AC-ID запасных деталей, хранящихся на складе, путем верификации аутентичности маркировок на хранимых деталях и проверки совпадения серийного номера компонента из цифровой 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, то есть 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 цифровой защитной маркировке цифрового идентификационного документа компонента самолета для этого компонента, и соответствующие контрольные данные уникальной физической подписи UPS вычисляются (например, путем взятия хеш-значения характеристических цифровых данных CDD, то есть UPS = H(CDD)) и могут также быть частью цифровых данных компонента D. 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 ЦП компьютера). Затем специалист (или ЦП его компьютера, если он подходящим образом запрограммирован) сравнивает полученные CDD^c с копией контрольных CDD, сохраненных в памяти компьютера: в случае "обоснованного" совпадения $CDD^c \approx CDD$ (то есть в пределах некоторого заранее определенного критерия допустимых ошибок) защитная маркировка на основе материала и, следовательно, компонент считаются подлинными.

Как упомянуто выше, копия контрольных характеристических цифровых данных CDD, вместо того, чтобы храниться в памяти компьютера специалиста, является частью цифровых данных D, включенных в цифровую защитную маркировку в цифровом идентификационном документе компонента самолета AC-ID:A компонента A, и может быть получена путем непосредственного считывания цифровой защитной маркировки. Затем специалист может считать потенциальные CDD^c на цифровой 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 возможно дополнительно верифицировать аутентичность копию цифрового идентификационного документа компонента самолета AC-ID:A_{125}, например, относительно оригинального защищенного цифрового файла. В действительности, если специалист, ответственный за операции контроля (или ремонта), имеет доступ к цифровому файлу AC-ID:A_{125} на своем компьютере (который может быть, например, смартфоном, запрограммированным подходящим образом), он может проверить соответствие цифровых данных компонента данным оригинального документа путем выполнения следующих операций:

считывания цифровых данных компонента D_{125} и цифрового ключа верификации k_{125} на цифровой защитной маркировке 310 цифрового идентификационного документа компонента AC-ID:A_{125};

получения контрольного значения R пакета, соответствующего документу AC-ID:A_{125}; это контрольное значение может уже быть в памяти компьютера или его можно получить посредством канала связи из базы данных, хранящей контрольные значения пакета цифровых идентификационных документов компонентов самолета, если компьютер оснащен блоком связи, путем отправки запроса, содержащего, например, (уникальный) серийный номер компонента или просто ключ k_{125}, считываемый на цифровой защитной маркировке 310, и приема обратно соответствующего контрольного значения пакета 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 пакета R^c (посредством запрограммированной односторонней хеш-функции H и цифровой подписи конкатенации цифровых подписей) в виде цифровой подписи посредством хеш-функции H конкатенации значения листового узла x_{125} и значений узлов, указанных в цифровом ключе верификации k_{125} (согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева); и

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

Согласно вышеприведенному подробному описанию настоящее изобретение явно совместимо с операциями автономной и локальной проверки для верификации аутентичности защищенного цифрового файла или соответствия данных копии защищенного цифрового файла относительно данных, связанных с оригинальным защищенным цифровым файлом. Однако настоящее изобретение также совместимо с процессом верификации в режиме "онлайн", например, путем приема (через канал связи) контрольного значения пакета (или корневой цифровой подписи) из внешнего источника (например, сервера или блокчейна) или выполнения некоторых или всех этапов вычисления, включающих одностороннюю функцию или конкатенацию цифровых подписей 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 цифрового файла, принадлежащего к пакету множества оригинальных цифровых файлов, от подделки или фальсификации, при этом каждый оригинальный цифровой файл включает свои собственные цифровые данные, отличающийся тем, что способ включает этапы

для каждого оригинального цифрового файла пакета вычисления посредством односторонней функции связанной с цифровым файлом подписи его цифровых данных;

формирования дерева на основании множества вычисленных подписей цифровых файлов для оригинальных цифровых файлов пакета, содержащего узлы, расположенные согласно заданной упорядоченности узлов в дереве, при этом указанное дерево содержит уровни узлов, начиная от листовых узлов, соответствующих множеству подписей цифровых файлов, соответственно, связанных с множеством оригинальных цифровых файлов в пакете, 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 корневой контрольной цифровой подписи, то есть цифровой подписи посредством односторонней функции конкатенации цифровых подписей узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

связывания с заданным оригинальным цифровым файлом соответствующего цифрового 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 подписи заданного оригинального цифрового файла, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский уровень в дереве, что и предыдущий такой же

родительский узел, рассмотренный на предшествующем уровне;

предоставления в распоряжение пользователя контрольной корневой цифровой подписи дерева и

включения в заданный оригинальный цифровой файл соответствующей машиночитаемой цифровой защитной маркировки, содержащей представление его цифровых данных и его соответствующего цифрового ключа верификации, при этом машиночитаемая цифровая защитная маркировка представлена в виде двухмерного штрих-кода,

тем самым получая маркированный оригинальный цифровой файл, цифровые данные 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 маркированный оригинальный цифровой файл дополнительно содержит данные по доступу к корневому узлу, включенные в него и содержащие информацию, достаточную для обеспечения доступа пользователю к контрольной корневой цифровой подписи корневого узла дерева, соответствующего пакету оригинальных цифровых файлов, при этом указанная информация является ссылкой на интерфейс доступа, выполненный с возможностью приема от пользователя корневого запроса, содержащего цифровые данные или подпись цифрового файла, получаемые из цифровой защитной маркировки маркированного оригинального цифрового файла, 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

виртуальный цифровой файл считается принадлежащим к пакету оригинальных цифровых файлов, при этом указанный виртуальный цифровой файл включает его собственные виртуальные цифровые данные и связанную с виртуальным цифровым файлом подпись, получаемую посредством односторонней функции виртуальных цифровых данных, при этом указанный виртуальный цифровой файл не является реальным, а используется только для генерирования связанной с виртуальным цифровым файлом подписи из его виртуальных цифровых данных; и

контрольная корневая цифровая подпись, связанная с указанным пакетом оригинальных цифровых файлов, вычислена из дерева, имеющего все подписи оригинальных цифровых файлов пакета, включающие подпись виртуального цифрового файла, в виде листовых узлов.

5. Способ по любому из пп.1-4, отличающийся тем, что дополнительные цифровые данные, соответствующие цифровым данным, связанным с маркированным оригинальным цифровым файлом, 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 или подпись цифрового файла, получаемые из цифровой защитной маркировки маркированного оригинального цифрового файла, и отправки обратно соответствующих дополнительных цифровых данных.

6. Способ по любому из пп.1-5, отличающийся тем, что цифровые данные маркированного оригинального цифрового файла включают контрольные характеристические цифровые данные соответствующей уникальной физической характеристики связанного объекта или человека.

7. Способ по п.6, отличающийся тем, что уникальная физическая характеристика связанного объекта или человека представляет собой, соответственно, характеристику защитной маркировки на основе материала, нанесенной на связанный объект или идентифицирующий биометрический признак связанного человека.

8. Способ по любому из пп.1-7, отличающийся тем, что в случае распределения цифровых данных соответственных оригинальных цифровых файлов пакета между заданными полями, общими для всех цифровых файлов пакета, и конкретные цифровые данные, относящиеся к этим полям, не включены в цифровые данные, но сгруппированы в отдельный блок данных полей, связанный с пакетом, и при этом:

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

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

9. Способ верификации аутентичности цифрового файла, защищенного согласно способу по любому из пп.1-7, или соответствия копии такого защищенного цифрового файла относительно оригинального файла, отличающийся тем, что способ включает этапы, при обработке тестового файла, представляющего собой указанный цифровой файл или указанную копию цифрового файла, посредством блока обра-

ботки, подключенного к памяти

сохранения в памяти тестового файла;

считывания представления цифровых данных и цифрового ключа верификации на цифровой защитной маркировке сохраненного тестового файла и извлечения, соответственно, соответствующих тестовых цифровых данных и тестового цифрового ключа верификации из указанного считанного представления;

сохранения в памяти контрольной корневой цифровой подписи корневого узла дерева пакета оригинальных цифровых файлов 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 и связанного тестового цифрового ключа верификации сохраненной контрольной корневой цифровой подписи путем осуществления этапов

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

извлечения из последовательности цифровых подписей в тестовом цифровом 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 цифровом 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, цифровые данные тестового файла являются данными подлинного цифрового файла.

10. Способ по п.9, отличающийся тем, что маркированный оригинальный цифровой файл защищен согласно способу по п.8, 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 цифровой защитной маркировке на тестовом файле, включает вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных и сохраненного блока данных полей.

11. Способ по любому из пп.9 и 10, отличающийся тем, что цифровой файл защищен путем сохранения контрольной корневой цифровой подписи в доступной для поиска корневой базе данных, открытой для пользователя, согласно способу по п.2, и блок обработки дополнительно подключен к блоку связи, выполненному 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 памяти.

12. Способ по любому из пп.9 и 10, отличающийся тем, что цифровой файл защищен согласно способу по п.3, блок обработки дополнительно подключен к блоку связи, выполненному с возможностью отправки и приема данных посредством канала связи, при этом способ включает предварительные этапы

считывания данных по доступу к корневому узлу, включенных в тестовый файл;

отправки блоком связи посредством канала связи корневого запроса в указанный интерфейс доступа, содержащего цифровые данные или цифровую подпись указанных цифровых данных, получаемых из цифровой защитной маркировки на тестовом файле, и приема обратно соответствующей контрольной корневой цифровой подписи связанного пакета; и

сохранения контрольной корневой цифровой подписи в памяти.

13. Способ по любому из пп.9-12, отличающийся тем, что цифровой файл защищен согласно способу по п.5 и устройство для формирования изображения дополнительно оснащено средствами связи, выполненными с возможностью отправки в интерфейс информационной базы данных запроса на информа-

цию, содержащего цифровые данные или подпись цифрового файла, получаемые из цифровой защитной маркировки тестового файла, и приема обратно соответствующих дополнительных цифровых данных.

14. Способ по любому из пп.9-13, отличающийся тем, что цифровой файл защищен согласно способу по любому из пп.6 и 7 и устройство для формирования изображения дополнительно оснащено датчиком, выполненным с возможностью обнаружения уникальной физической характеристики соответственно 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, 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, подлинному объекту или человеку, действительно связанному с подлинным цифровым файлом.

15. Цифровой файл, принадлежащий к пакету множества оригинальных цифровых файлов и защищенный согласно способу по любому из пп.1-8, при этом каждый оригинальный цифровой файл пакета имеет свои собственные цифровые данные и соответствующий цифровой ключ верификации, указанный пакет имеет соответствующую контрольную корневую цифровую подпись, при этом файл содержит машиночитаемую защитную маркировку, включающую представление его цифровых данных и его ключа верификации.

16. Цифровой файл по п.15, отличающийся тем, что цифровые данные включают контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека.

17. Цифровой файл по п.16, отличающийся тем, что уникальная физическая характеристика связанного объекта представляет собой характеристику защитной маркировки на основе материала, нанесенной на связанный объект.

18. Система верификации аутентичности цифрового файла или соответствия копии такого цифрового файла относительно маркированного оригинального цифрового файла, принадлежащего к пакету оригинальных цифровых файлов, защищенных согласно способу по любому из пп.1-7, 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 пакету оригинальных цифровых файлов, и одностороннюю функцию для вычисления цифровой подписи цифровых данных и конкатенации цифровых подписей согласно упорядоченности узлов дерева и упорядоченности конкатенации дерева, запрограммированную в блоке обработки, при этом указанная система выполнена с возможностью

сохранения в памяти тестового файла, представляющего собой указанный цифровой файл или указанную копию цифрового файла;

считывания представления цифровых данных и цифрового ключа верификации на цифровой защитной маркировке сохраненного тестового файла и извлечения, соответственно, соответствующих тестовых цифровых данных и тестового цифрового ключа верификации из указанного считанного представления;

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

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

извлечения из последовательности цифровых подписей в тестовом цифровом 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 цифровом 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 цифровые данные тестового файла являются данными подлинного цифрового файла.

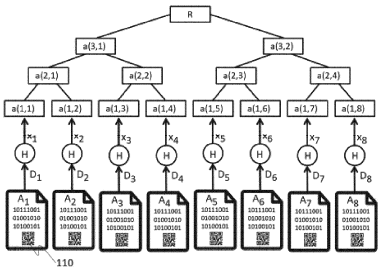
19. Система по п.18, отличающаяся тем, что маркированный оригинальный цифровой файл защищен согласно способу по п.8, память блока обработки дополнительно сохраняет связанный блок данных полей, и при этом запрограммированные операции вычисления тестовой цифровой подписи, соответствующей тестовому листовому узлу в тестовом дереве, соответствующем цифровой защитной маркировке тестового файла, включают вычисление с помощью односторонней функции цифровой подписи конкатенации извлеченных тестовых цифровых данных и сохраненного блока данных полей.

20. Система по любому из пп.18 и 19, отличающаяся тем, что маркированный оригинальный цифровой файл принадлежит к пакету оригинальных цифровых файлов, защищенных согласно способу по любому из пп.6 и 7, при этом система дополнительно оснащена датчиком, подключенным к блоку обработки и выполненным с возможностью обнаружения уникальной физической характеристики связанного объекта или человека, и при этом блок обработки запрограммирован для извлечения соответствующих характеристических цифровых данных из сигнала обнаружения, принятого от датчика, система сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике связанного объекта или человека, при этом система дополнительно выполнена с возможностью

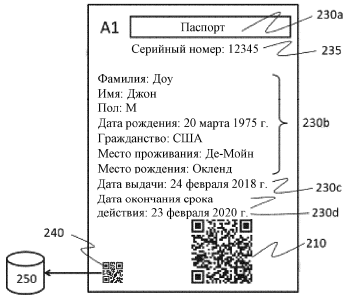
обнаружения с помощью датчика уникальной физической характеристики субъекта, представляющего собой указанный связанный объект или человека, и извлечения соответствующих потенциальных характеристических цифровых данных CDD^c;

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

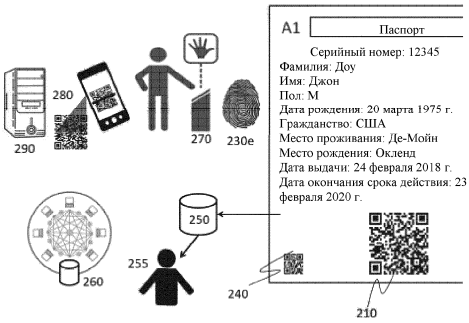
в случае схожести потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD, при условии заданного критерия допустимого отклонения, доставки указания того, что субъект считается подлинным.



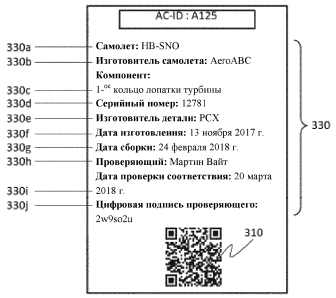
Фиг. 1



Фиг. 2A


A1
Паспорт
Серийный номер: 12345
Фамилия: Доу
Имя: Джон
Пол: М
Дата рождения: 20 марта 1975 г.
Гражданство: США
Место проживания: Де-Мойн
Место рождения: Окленд
Дата выдачи: 24 февраля 2018 г.
Дата окончания срока действия: 23 февраля 2020 г.
280
290
270
230e
250
255
260
240
210

Фиг. 2B


AC-ID : A125
330a Самолет: HB-SNO
330b Изготовитель самолета: AeroABC
Компонент:
330c 1-ое кольцо лопатки турбины
330d Серийный номер: 12781
330e Изготовитель детали: PCX
330f Дата изготовления: 13 ноября 2017 г.
330g Дата сборки: 24 февраля 2018 г.
330h Проверяющий: Мартин Вайт
Дата проверки соответствия: 20 марта
330i 2018 г.
330j Цифровая подпись проверяющего:
2w9so2u
330
310

Фиг. 3