(19) Евразийское патентное ведомство

(11) 040639 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.07.08

(21) Номер заявки
202190068

(22) Дата подачи заявки
2019.06.03

(51) Int. Cl. ***G06F 21/64*** (2013.01)
H04L 9/32 (2006.01)

(54) ЗАЩИТА ЦИФРОВОГО ФАЙЛА ОТ ПОДДЕЛКИ

(31) **18178628.6**
(32) **2018.06.19**
(33) **EP**
(43) **2021.04.08**
(86) **PCT/EP2019/064376**
(87) **WO 2019/243034 2019.12.26**

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

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

(74) Представитель:
Рыбина Н.А. (RU)

(56) AHTO BULDAS ET AL.: "Efficient Record-Level Keyless Signatures for Audit Logs", INTERNATIONAL ASSOCIATION FOR CRYPTOLOGIC RESEARCH, vol. 20140718:122633, 15 July 2014 (2014-07-15), pages 1-13, XP061016649, paragraph [04.2], paragraph [02.1]

BENALOH J. ET AL.: "ONE-WAY ACUMULATORS: A DECENTRALIZED ALTERNATIVE TO DIGITAL SIGNATURES (EXTENDED ABSTRACT)", ELECTRONIC PUBLISHING, ARTISTIC IMAGING, AND DIGITAL TYPOGR; [LECTURE NOTES IN COMPUTER SCIENCE, ISSN 0302-9743], SPRINGER VERLAG, DE, vol. 765, 23 May 1993 (1993-05-23), pages 274-285, XP008066935, ISBN: 978-3-540-24128-7 paragraph [0005]

US-A1-2012125997

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

040639 B1

040639 B1

Область техники, к которой относится изобретение

Настоящее 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 недостаточным решением, поскольку фальсификаторы могут легко скопировать такие номера или цифровые водяные знаки.

Ahto Buldas et al.: "Efficient Record-Level Keyless Signatures for Audit Logs", International Association for Cryptologic Research, выпуск 20140718:122633, стр. 1-13, от 15 июля 2014 г., раскрывает схему подписи журнала записей, которая позволяет верифицировать целостность всего журнала записей и представление любой записи, а также краткое доказательство того, что запись не была изменена с момента подписывания журнала записей, причем журнал записей представляет собой упорядоченную последовательность блоков, где каждый блок, в свою очередь, представляет собой упорядоченную последовательность записей.

В документе US 2012125997 A1 раскрыт подход, который фактически использует технологию цифровой подписи инфраструктуры открытых ключей (PKI) и штрих-кода для предоставления паспорта, аутентичность и целостность данных которого могут быть подтверждены в печатной форме. Есть инструмент штрихового кодирования, который включает компонент извлечения данных; компонент конкатенации данных; компонент генерирования цифровой подписи и компонент генерирования штрих-кода. Также есть инструмент для считывания штрих-кода, который включает считывание символов штрих-кода идентификационных данных и цифровой подписи с использованием считывателя штрих-кода; отображение идентификационных данных и цифровой подписи на устройстве для отображения; верификацию электронной подписи и отображение результатов верификации на устройстве для отображения. 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 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 цифрового файла, защищенного согласно настоящему изобретению, и соответствия содержимого его цифровых данных содержимому подлинного цифрового файла.

Краткое описание изобретения

Один из аспектов настоящего изобретения относится к способу защиты заданного оригинального цифрового файла из пакета множества оригинальных цифровых файлов от подделки или фальсификации, при этом каждый оригинальный цифровой файл пакета содержит 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;

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

определения ключа верификации цифрового файла, соответствующего подписи указанного заданного оригинального цифрового файла, посредством частичного одностороннего сумматора других подписей цифровых файлов, используемых для вычисления контрольной агрегированной цифровой подписи, в результате чего потенциальная подпись цифрового файла соответствует подписи оригинального цифрового файла пакета, в случае извлечения контрольной агрегированной цифровой подписи из односторонней функции указанной потенциальной подписи цифрового файла и соответствующего ключа верификации цифрового файла; и

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

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

Контрольная агрегированная цифровая подпись, связанная с пакетом оригинальных цифровых фай-

лов, может быть либо опубликована в среде, открытой для пользователя, либо сохранена в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, либо сохранена в блокчейне, либо сохранена в базе данных, защищенной блокчейном, открытой для пользователя.

Маркированный оригинальный цифровой файл дополнительно может включать данные по доступу к агрегированным подписям, содержащие информацию, достаточную для получения доступа к контрольной агрегированной цифровой подписи, соответствующей пакету оригинальных цифровых файлов, при этом указанная информация представляет собой ссылку в интерфейс сбора агрегированных подписей, соответственно, одного из следующего:

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

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

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

Согласно настоящему изобретению можно считать, что виртуальный цифровой файл принадлежит к пакету оригинальных цифровых файлов, при этом указанный виртуальный цифровой файл имеет соответствующие виртуальные цифровые данные и связанную с виртуальным цифровым файлом подпись, получаемую посредством односторонней функции его виртуальных цифровых данных, при этом указанный виртуальный цифровой файл не является реальным, а используется только для генерирования связанной с виртуальным цифровым файлом подписи из соответствующих виртуальных цифровых данных; и контрольная агрегированная цифровая подпись, связанная с указанным пакетом оригинальных файлов, вычислена из всех подписей оригинальных цифровых файлов пакета, включающих подпись виртуального цифрового файла, посредством одностороннего сумматора.

Односторонняя функция может представлять собой хеш-функцию, а 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 соответствующие данные подписи цифрового файла, получаемые из цифровой защитной маркировки маркированного оригинального цифрового файла, и отправки обратно соответствующих дополнительных цифровых данных.

Более того, цифровые данные маркированного оригинального цифрового файла могут включать контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека.

Другой аспект настоящего изобретения относится к способу верификации аутентичности цифрового файла, защищенного согласно вышеуказанному способу, 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 ключа верификации тестового файла на цифровой защитной маркировке в сохраненном тестовом файле и извлечения, соответственно, соответствующих цифровых данных и ключа верификации тестового файла из указанного считанного представления;

сохранения в памяти контрольной агрегированной цифровой подписи соответствующего пакета цифровых файлов и программирования в блоке обработки односторонней функции и одностороннего сумматора; верификации действительного соответствия извлеченных цифровых данных и ключа вери-

фикации тестового файла сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов:

вычисления цифровой подписи извлеченных цифровых данных с помощью односторонней функции; вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных и извлеченного ключа верификации тестового файла с помощью одностороннего сумматора; и

проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего в случае совпадения указанных агрегированных цифровых подписей цифровые данные тестового файла являются данными подлинного оригинального цифрового файла.

Способ верификации, в котором цифровой файл защищен путем сохранения контрольной агрегированной цифровой подписи, связанной с пакетом оригинальных цифровых файлов, в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, и в котором блок обработки дополнительно подключен к блоку связи, выполненному с возможностью отправки и приема обратно данных посредством канала связи, может включать предварительные этапы:

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

сохранения принятой агрегированной цифровой подписи в памяти.

В указанном способе верификации, в котором маркированный оригинальный цифровой файл дополнительно включает данные по доступу к агрегированным подписям, содержащие информацию, достаточную для получения доступа к контрольной агрегированной цифровой подписи, соответствующей пакету оригинальных цифровых файлов, при этом указанная информация представляет собой ссылку в интерфейс сбора агрегированных подписей, и в котором блок обработки дополнительно подключен к блоку связи, выполненному с возможностью отправки и приема обратно данных посредством канала связи, может включать предварительные этапы:

считывания данных по доступу к агрегированным подписям, включенных в тестовом файле;

отправки блоком связи посредством канала связи запроса на агрегированную подпись в указанный интерфейс сбора агрегированных подписей, содержащего цифровые данные или цифровую подпись указанных цифровых данных, получаемые из цифровой защитной маркировки в тестовом файле, и

приема обратно соответствующей контрольной агрегированной цифровой подписи связанного пакета; и сохранения принятой агрегированной цифровой подписи в памяти.

В вышеуказанном способе верификации оригинальный цифровой файл может быть защищен дополнительными цифровыми данными, хранящимися в доступной для поиска информационной базе данных, открытой для пользователя, посредством интерфейса информационной базы данных, как раскрыто выше, и блок обработки может быть дополнительно подключен к средствам связи, выполненным с возможностью отправки в интерфейс информационной базы данных запроса на информацию, содержащего цифровые данные или соответствующую подпись цифрового файла, получаемые из цифровой защитной маркировки в тестовом файле, и приема обратно соответствующих дополнительных цифровых данных.

Более того, в вышеуказанном способе верификации, в случае если цифровые данные маркированного оригинального цифрового файла включают контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека, и блок обработки подключен к датчику, выполненному с возможностью обнаружения уникальной физической характеристики связанного объекта или человека, блок обработки запрограммирован для извлечения соответствующих цифровых данных уникальной физической характеристики из сигнала обнаружения, принятого от датчика, блок обработки может дополнительно хранить в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике связанного объекта или человека, и способ включает дополнительные этапы, при рассматривании субъекта, представляющего собой, соответственно, указанный связанный объект или человека: обнаружения уникальной 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, при условии заданного критерия допустимого отклонения, субъект считается подлинным.

Другой аспект настоящего изобретения относится к маркированному цифровому файлу, принадлежащему к пакету множества оригинальных цифровых файлов и защищенному от подделки или фальсификации согласно вышеописанному способу защиты, при этом каждый оригинальный цифровой файл пакета имеет свои собственные цифровые данные, указанный пакет имеет соответствующую контрольную агрегированную цифровую подпись, маркированный цифровой файл содержит машиночитаемую цифровую защитную маркировку, включающую представление его цифровых данных и соответствующего ключа верификации цифрового файла. Более того, цифровые данные маркированного цифрового

файла могут дополнительно включать контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека.

Согласно еще одному аспекту настоящее изобретение относится к системе верификации аутентичности маркированного оригинального цифрового файла, защищенного согласно вышеупомянутому способу защиты, или соответствия копии такого цифрового файла относительно оригинального файла, при этом система содержит блок обработки с памятью, память сохраняет контрольную агрегированную цифровую подпись соответствующего пакета цифровых файлов и одностороннюю функцию и односторонний сумматор, запрограммированные в блоке обработки, при этом система выполнена с возможностью получения тестового файла, представляющего собой указанный цифровой файл или копию цифрового файла, и сохранения полученного тестового файла в памяти; считывания представления цифровых данных и ключа верификации тестового файла на цифровой защитной маркировке в сохраненном тестовом файле и извлечения, соответственно, соответствующих цифровых данных и ключа верификации тестового файла из указанного считанного представления; верификации действительного соответствия извлеченных цифровых данных и ключа верификации тестового файла сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов, запрограммированных в блоке обработки: вычисления цифровой подписи извлеченных цифровых данных с помощью односторонней функции; вычисления потенциальной агрегированной цифровой подписи из вычисленной цифровой подписи извлеченных цифровых данных и извлеченного ключа верификации тестового файла с помощью одностороннего сумматора; и проверки совпадения полученной потенциальной агрегированной цифровой подписи с сохраненной контрольной агрегированной цифровой подписью, в результате чего в случае совпадения указанных агрегированных цифровых подписей цифровые данные тестового файла являются данными подлинного оригинального цифрового файла, и система выполнена с возможностью доставки указания того, что цифровые данные на тестовом файле являются данными подлинного оригинального цифрового файла.

Такая система верификации цифрового файла, защищенного согласно вышеупомянутому способу защиты, или соответствия копии такого цифрового файла относительно оригинального файла, в случае если цифровые данные маркированного оригинального цифрового файла включают контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека, может быть 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, 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.

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

Краткое описание чертежей

На фиг. 1 представлен схематический вид общего способа защиты пакета цифровых файлов согласно настоящему изобретению;

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

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

на фиг. 3 - пакет компонентов 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_2, A_3, ..., 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".

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). На фиг. 1 также показан "виртуальный цифровой файл" A_v, который является необязательным средством программного обеспечения, которое может быть включено для обеспечения кодирования выбранных данных. Это объясняется далее. Исключительно для примера предполагается, что виртуальный цифровой файл A_v включен и будет рассматриваться ниже как другие (реальные) цифровые файлы A_1, A_2, A_3, ..., поскольку он может обрабатываться практически таким же образом (хотя он не соответствует реальному файлу, например хранится в памяти). Конечно, множество виртуальных цифровых файлов A_{v1}, A_{v2}, ..., A_{vk} можно использовать для кодирования цифровых данных и создания более надежных цифровых подписей (см. ниже).

Для каждого цифрового файла A_1, A_2, A_3, ..., A_v соответственные цифровые данные D_1, D_2, D_3, ..., D_v связаны или извлечены (или в случае виртуального цифрового файла A_v созданы) с помощью любого пригодного способа. Эти данные могут представлять собой некоторую меру физических характеристик, текстовые данные, такие как заполненная форма или информация о продукте, серийный номер или другой идентификатор, указания содержимого, цифровое представление изображения или любая другая информация, которую разработчик системы решает связать с файлом. Цифровые данные D_i цифрового файла A_i могут быть извлечены из читаемого человеком представления данных (например, буквенно-цифровых данных) посредством считывателя, выполненного с возможностью создания соответствующего файла цифровых данных. Дополнительные цифровые данные могут быть связаны с извлеченными данными для создания цифровых данных D_i, содержащихся в файле A_i.

Для виртуального цифрового файла A_v связанные цифровые данные D_v могут включать, например, идентификационный номер пакета, (псевдо) рандомный номер с целью увеличения защиты путем увеличения энтропии данных, информации о дате и/или времени и т.д. Еще одной формой связанных цифровых 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 цифрового файла его соответственные цифровые данные D_1, D_2, D_3, ..., D_v предпочтительно преобразовываются математическим путем, так что они, по существу, скрыты, хотя это не является абсолютным требованием для любого варианта осуществления. Это преобразование, применяемое к цифровым данным D_i цифрового файла A_i, служит для создания соответствующей цифровой подписи x_i. Эту цифровую подпись получают посредством односторонней функции (т.е. функции, которую легко вычислить, но трудно инвертировать, см. S. Goldwasser and M. Bellare "Lecture Notes on Cryptography", MIT, июль 2008 г., http://www-cse.ucsd.edu/users/mihir).

Одним из таких выгодных преобразований является, например, применение хеш-функции H( ) = hash( ) к цифровым данным, которая обычно имеет свойство возвращать выходные данные известной длины в битах независимо от размера входных данных: этот технический эффект особенно полезен для создания цифровой подписи цифровых данных, связанных с цифровым файлом, независимо от размера связанных 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, т.е. вероятность того, что две разные группы входных данных приведут к одним и тем же выходным данным, ничтожна. Как будет понятно из приведенного ниже описания, это также не является требованием настоящего изобретения, хотя оно выгодно по тем же причинам, что и в других приложениях. Как показано на фиг. 1, значения x_1, x_2, x_3, ..., x_v представляют собой хеш-значения, т.е. связанные с цифровыми файлами подписи, соответственных цифровых данных цифровых файлов, т.е. $x_j = H(D_j)$, для j=1, ..., v. Для краткости X (заглавная буква) используется в данном случае и на фиг. 1 для обозначения набора хешированных значений данных; таким образом, $X = (x_1, x_2, ..., x_v)$ (если включен виртуальный цифровой файл A_v; в противном случае элемент x_v можно опустить).

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

Агрегированную цифровую подпись или значение пакета B затем вычисляют по X посредством (квази-коммутативного) одностороннего сумматора (см. статью Josh Benaloh and Michael de Mare "One-Way Accumulators: A Decentralized Alternative to Digital Signatures", Advances in Cryptology - Eurocrypt' 93, LNCS, выпуск 765, стр. 274-285, Springer-Verlag, 1993 г.). В общем, для набора □ подписей x_1, x_2, ..., $.x_\mu$ (возможно в том числе подписей одного или более виртуальных цифровых файлов), соответствующее

суммарное значение $f(x_1, x_2, ..., x_\mu)$, сокращено как $f(X)$ с $X = (x_1, x_2, ..., x_\mu)$, заданное односторонним сумматором f, представляет собой

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

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

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

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

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

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

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

с ключом верификации $k_1 = (x_2 \otimes x_3 \otimes \dots \otimes x_\mu) = f(X^1)$.

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

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

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

Для каждого цифрового файла A_i компилируется соответствующая информация о верификации V_i, которая кодируется в некоторой форме машиночитаемой защитной маркировки 110, которая затем связывается с соответственным цифровым файлом.

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

Дополнительные цифровые данные могут дополнительно быть связаны с цифровым файлом и могут включать, например, значение пакета B или любую другую информацию, которую разработчик системы выбирает включить, как, например, серийный номер файла, идентификатор пакета, информация о дате/времени, название содержимого, URL-адрес, который указывает на другую онлайн-информацию, связанную либо с отдельным файлом (например, цифровое изображение соответствующего изделия и т.д.), либо с пакетом, либо с номером 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 верификации k_i оригинального цифрового файла A_i и включения (т.е. посредством кодирования или любого выбранного представления данных) вместе с соответствующими цифровыми данными D_i в машиночитаемую цифровую защитную маркировку 110, добавленную к оригинальному цифровому файлу, полученный в результате маркированный оригинальный цифровой файл и связанные с ним цифровые данные действительно защищены от подделки и фальсификации. Преимущество настоящего изобретения состоит в том, что в цифровую защитную маркировку не включают ключ кодирования/декодирования.

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

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

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

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

В одном иллюстративном варианте осуществления функция одностороннего сумматора f(X) выбрана как простое (коммутативное) умножение по модулю, т.е. f(x) = x mod m, и f(x, y) = x⊗y = x * y mod m.

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

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

т.е. $f(X) = x_1 \otimes x_2 \otimes \ldots \otimes x_\mu$, где m представляет собой модуль, а X соответствует μ подписям □ цифровых файлов в пакете $X = (x_1, \ldots, x_\mu)$. Умножение по модулю - это очень простой пример одностороннего сумматора (не только квазикоммутативного, но и коммутативного), хотя и не надежного. Таким образом, на словах значение пакета B = f(X) вычисляют путем умножения всех хеш-значений цифровых файлов x_i вместе, а затем взятия остатка данного произведения после деления на модуль m. В некоторых случаях это может привести к получению непрактично большого произведения. Например, предположим, что в пакете 1000 цифровых файлов, и каждое хеш-значение x_i имеет длину 256 бит (как получено с помощью хеш-функции SHA-256). Можно было бы выполнить 999 умножений и сохранить результат, а затем выполнить деление на m для получения остатка, но это неудобно и потребовало бы ненужных вычислительных усилий в виде сохранения значений без усечения.

Вместо этого система может использовать свойство операций по модулю, что результат можно вычислять несколько раз, попарно, как показано в следующем псевдокоде:

B = 1

For j = 1 to μ

B: = [B * x(j)] mod m

Следующее j

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

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

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

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

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

3 mod 10 = 3,

6 mod 10 = 6 и

8 mod 10 = 8, но

B = 3×6×8 mod 10 = 144 mod 10 = 4.

Если ключ верификации для первого цифрового файла задан как 6×8 mod 10 = 8, а значение пакета B = 4, чтобы угадать хеш-значение 3 цифровых данных, все равно нужно будет угадать набор из десяти возможностей. Сложность, конечно, будет расти по мере увеличения длины в битах x_i и m. Специально для пакетов из более чем десяти цифровых файлов или более 100 цифровых файлов, где m установлено в виде $m > \max_i(x_i)$, например, до максимального значения, которое может быть представлено для заданной длины в битах (такой как 256 для реализации, которая использует хеш-функцию SHA-256), злоумышленнику будет неэффективно пытаться вычислительным образом подделать хеш-значение для каждой подписи пакета цифровых файлов, особенно в реализациях, в которых важность или даже финансовая ценность каждого цифрового файла в пакете слишком мала, чтобы оправдать попытку такой атаки. Другими словами, используя этот вариант осуществления, нет смысла пытаться подделать информацию, закодированную в маркировке.

Преимущество $m > \max(x_1, x_2, \ldots, x_\mu)$ выбора состоит в том, что для всех хеш-значений ($x_i$mod m =

x_i) существует свойство эквивалентности, но это не обязательно. Скорее может быть выбрано любое значение, в частности, для обеспечения желаемой длины в битах для B. Также необязательно, чтобы m было постоянным во всех реализациях настоящего изобретения или даже для всех пакетов. В качестве одного из примеров администратор, поставщик услуг и т.д. может выбрать разный модуль m для разных пакетов. Они могут храниться в базе данных либо в системе 100 защиты, либо где-либо еще, либо доставляться через какой-либо другой канал пользователю, например получателю цифровых файлов, чтобы только этот получатель мог легко верифицировать цифровые файлы на основании их цифровой защитной маркировки 110.

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

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

Пользователь, получатель 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 ключ верификации k_1 (и любую другую информацию, которая могла быть закодирована в цифровой защитной маркировке). Примером считывателя является компьютер с дисплеем. 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 подписи цифрового файла, в данном случае это хеш-функция H( ), а затем выполнить операцию $x_1 = H(D_1)$ для получения полных данных (x_1, k_1), необходимых для вычисления соответствующей потенциальной агрегированной цифровой подписи B^c. Пользователь может, например, безопасно принять одностороннюю функцию (например, используя пару открытого и личного ключей) или запросив ее у поставщика цифровых файлов или любого другого объекта, который создал подписи и ключи или уже запрограммировал их в блок обработки считывателя пользователя.

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

Используя модуль m, пользователь может затем вычислить потенциальную агрегированную цифровую подпись $B^c = k_1 \otimes x_1$, которая затем должна быть равна доступному (или опубликованному) значению B: это значение могло быть ранее получено пользователем и/или уже сохранено в памяти блока обработки считывателя, это также может быть значение, которое получатель запрашивает и принимает от системного администратора любым известным способом. При совпадении потенциальных B^c и доступных агрегированных цифровых подписей B данное вычисление затем верифицирует информацию в защитной цифровой маркировке 110 и подтверждает, что цифровой файл A_1 принадлежит правильному пакету.

Ссылка для доступа к значению пакета B для пакета, соответствующему цифровому файлу A_1, может быть включена в цифровую защитную маркировку 110 (например, веб-адрес, если B можно извлечь из соответствующего веб-сайта), хотя это не предпочтительный вариант.

В некоторых реализациях получатели цифрового файла A_i могут иметь возможность "визуально" извлекать данные, соответствующие цифровым данным D_i, непосредственно из цифрового файла. Например, данные могут быть текстовыми, такими как серийный номер, или являться текстом в описательном письме, или некоторым буквенно-цифровым кодированием и читаться человеком из самих цифровых файлов. Получателям цифровых файлов также может быть предоставлено пригодное программное обеспечение, такое как модуль в устройстве для считывания, таком как смартфон, компьютер или планшет, который либо вводит данные, либо считывает данные, а затем вычисляет $x_i = H(D_i)$ для текущего цифрового файла. Например, с помощью цифровой защитной маркировки 110 на цифровом файле A_1, представляющей собой стандартный QR-код, пользователь сможет легко получить путем декодирования QR-кода с помощью компьютера, используя стандартное приложение для декодирования QR-кода, запущенное на компьютере, цифровые данные D_1 и ключ верификации цифрового файла k_1, приложение

для верификации на компьютере пользователя затем сможет вычислить $x_1 = H(D_1)$ и $B^c = f(X) = f(x_1 \otimes X^1) = x_1 \otimes f(X^1) = f(X^1) \otimes x_1 = k_1 \otimes x_1$, а также сравнить данное значение с доступным значением пакета B, как раскрыто выше. Например, если оператор $\otimes$ соответствует умножению по модулю, то $k_1 \otimes x_1 = (k_1 * x_1) \bmod m$.

Предпочтительно агрегированная цифровая подпись (т.е. значение пакета) B хранится в доступной для поиска базе данных агрегированных подписей, к которой может получить доступ (через канал связи) пользователь с помощью своего компьютера, оснащенного устройством для связи, как это имеет место с приведенным выше примером смартфона. Пользователь, которому необходимо верифицировать цифровой файл A_1, может просто отправить запрос со своего смартфона на адрес базы данных через интерфейс сбора подписей базы данных, запрос, содержащий цифровые данные D_1, считанные на цифровой защитной маркировке 110, в A_1 (или вычисленную подпись цифрового файла $x_1 = H(D_1)$), что позволяет извлечь соответствующее значение пакета B, а интерфейс сбора данных вернет агрегированную цифровую подпись B на смартфон (или компьютер). База данных может быть защищена блокчейном, чтобы усилить неизменность сохраненных агрегированных цифровых подписей. Преимущество настоящего изобретения заключается в том, чтобы установить связь между физическим объектом, т.е. оригинальным цифровым файлом (например, хранящимся в памяти), и его атрибутами, т.е. связанными цифровыми данными и его принадлежностью к пакету цифровых файлов, практически неизменно посредством соответствующей агрегированной 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 устройства для формирования изображения 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, представляющем 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, т.е. $UPS_i = H(CDD_i)$. Однако вместо этого можно использовать любое другое известное кодирование, например, чтобы иметь короткую подпись, можно использовать алгоритм цифровой подписи эллиптической кривой. В качестве очень упрощенного иллюстративного примера характеристических цифровых данных CDD_i, соответствующих уникальной физической характеристике 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, т.е. 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 подпи-

си 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, т.е. $UPS_i^c = H(CDD_i^c)$, совпадают с контрольными данными уникальной физической подписи UPS_i, сохраненными в памяти.

Пользователь может дополнительно проверить аутентичность принятого 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 $CDD_i^c \approx CDD_i$ (т.е. два цифровых данных согласуются с неким заданным критерием отклонения или схожести), цифровой файл A_i считается подлинным (т.е. 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, сохраненные 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 B 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, т.е. характеристические цифровые данные CDD_i и/или контрольные данные уникальной физической подписи UPS_i, хранятся в доступной для поиска базе данных, открытой для пользователя, где контрольные данные, относящиеся к цифровому файлу A_i, хранятся в связи, соответственно, с 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 D_i 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), т.е. маркировки, обладающей обнаруживаемым внутренним физическим или химическим свойством, которое очень трудно (если не невозможно) воспроизвести. Если пригодный датчик обнаруживает это внутреннее свойство маркировки, данная маркировка считается подлинной с высокой степенью достоверности, а следовательно, и 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 за-

щитная 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 соответствующей данным 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 τ, 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 ≈ 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.

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

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

что можно уменьшить, на основании квазикоммутативности f, к

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

где $\prod x_i$ обозначает произведение от i=1 до i=□ компонентов подписей цифровых файлов x_1, x_2, ... x_μ X, т.е. $\prod x_i = x_1 * x_2 * \ldots * x_\mu$. Действительно, квазикоммутативность этого одностороннего сумматора позволяет записать (для всех I и всех x, y): f(f(I;x),y) = f(f(I;y),x), где вышеупомянутое полученное в ре-

зультате преимущество заключается в том, что этап верификации не требует наличия дополнительной информации о упорядоченности подписей x_i.

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

Ключ верификации цифрового файла k_j, соответствующий подписи цифрового файла x_j цифровых данных D_j цифрового файла A_j из пакета □ цифровых файлов, вычисляют следующим образом:

$k_j = I^{(\prod xi/xj)} \bmod m$, где $(\prod x_i/x_j) = x_1 * x_2 * ... * x_{j-1} * x_{j+1} ... * x_\mu$, или где символическое обозначение

$k_j = I \otimes x_1 * x_2 * ... * x_{j-1} * x_{j+1} ... * x_\mu$.

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

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

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

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

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

Другой иллюстративный вариант осуществления настоящего изобретения относится к пакету цифровых биометрических идентификационных документов, например цифровые биометрические паспорта, как показано на фиг. 2. Каждый цифровой паспорт, как цифровой файл, связан с соответствующим человеком, т.е. с владельцем паспорта. Для ясности цифровые данные A_1 представлены на фиг. 2 в виде эквивалентной текстовой и буквенно-цифровой информации (т.е. 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.

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 (т.е. набор возможных ключей) больше, чем ее диапазон (т.е. количество различных индексов таблицы), он будет отображать несколько разных ключей в один и тот же индекс, что может привести к конфликтам: таких конфликтов можно избежать, когда размер 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. 2A 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 ("M"), 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, т.е. 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, соответст-

вующие 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 μ = 1024, связанные с паспортом цифровые данные D_j включают вышеупомянутые цифровые данные 230a-230e. 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.

На основе всех цифровых подписей цифровых паспортов в пакете вычисляют агрегированную цифровую подпись B с помощью одностороннего сумматора. Например, в этом варианте осуществления агрегированную подпись для пакета получают посредством вышеупомянутого одностороннего сумматора возведения в степень по модулю m, определяемого $f(x) = I^x \bmod m$, где I - заданное целое число, а m - модуль. Таким образом, агрегированную цифровую подпись B для пакета μ цифровых биометрических паспортов A_1, A_2, ..., A_μ (который может включать виртуальные цифровые паспорта), соответственные цифровые данные паспорта которого представляют собой D_1, D_2, ..., D_μ, и с соответствующими связанными с паспортами цифровыми подписями $x_1 = H(D_1)$, $x_2 = H(D_2)$, ..., $x_\mu = H(D_\mu)$, вычисляют для $X = (x_1, x_2, ..., x_\mu)$, как

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

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

На фиг. 2B проиллюстрирован процесс контроля защищенного цифрового биометрического паспорта A_1 согласно фиг. 2A, в котором цифровые данные 230 паспорта соответствуют 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 данные 240 по доступу к информации. Данные паспорта дополнительно содержат уникальный серийный номер 235, присвоенный органом, выдающим паспорт. Цифровая защитная маркировка 210 цифрового паспорта содержит информацию о верификации (D_1, k_1), в которой цифровые данные паспорта D_1 соответствуют данным 230a-230d паспорта, биометрическим данным 230e и уникальному серийному номеру 235, и ключ верификации k_1 соответствует $f(X^1)$, при обозначении $X^1 = (x_2, ..., x_{1024})$, $x_i = H(D_i)$ i =2, ..., 1024 и f представляет собой возведение в степень по модулю m (с заданными значениями целых чисел I и m).

Значение пакета B получают из всех цифровых подписей паспорта (x_1, ..., x_{1024}) как B = f(X), где (X = x_1, ..., x_{1024}). Вычисленной агрегированной цифровой подписи B можно дополнительно присваивать временную метку и хранить ее в блокчейне 260. В данном примере биометрические данные 230e соответственных владельцев цифровых биометрических паспортов пакета также хранятся в блокчейне 260 в связи, соответственно, с 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 цифровом паспорте. Органы, ответственные за контроль личности людей (например, полиция, таможня и т.д.), могут получить доступ к блокчейну 260 через канал связи ив этом иллюстративном варианте осуществления также имеют локальные хранилища для хранения (опубликованных) агрегированных цифровых подписей всех доставленных пакетов цифровых биометрических паспортов. В примере, показанном на фиг. 2B, информационная база 250 данных является локальной (т.е. непосредственно доступна органам, без необходимости использования общедоступной сети связи). Кроме того, эти органы оснащены сканерами 270 отпечатков пальцев для захвата отпечатков пальцев людей и вычисления соответствующих машиночитаемых представлений данных, характеризующих снятые отпечатки пальцев, т.е. биометрические данные 230e.

Во время проверки личности Джона Доу, скажем, сотрудником полиции или таможни сотрудник принимает защищенный цифровой биометрический паспорт A_1 Джона Доу, считывает и декодирует информацию о верификации (D_1, k_1), сохраненную в цифровой защитной маркировке 210 паспорта, посредством пригодного считывателя, который может представлять собой, например, подходящим образом запрограммированный компьютер 290, при этом компьютер подключен к локальным хранилищам 250. Если у Джона Доу есть только материальный документ, например бумажный, биометрический паспорт (маркированный печатной защитной маркировкой, соответствующей цифровой защитной маркировке 210), сотрудник может получить связанный цифровой биометрический паспорт A_1, сняв цифровое изображение документа с помощью сканера 280, подключенного к компьютеру 290, обработав цифровое изображение для преобразования его содержимого данных в соответствующие цифровые данные и сохранив извлеченные цифровые данные в компьютер 290 в виде цифрового файла, соответствующего цифровому биометрическому паспорту A_1 Джона Доу. После считывания цифровых данных паспорта D_1 и ключа верификации k_1 и отправки их на компьютер 290, определенное приложение (с запрограммированной хеш-функцией H и односторонним сумматором), запущенное на компьютере 290, вычисляет цифровую подпись паспорта x_1 (как x_1 =H(D_1)) и потенциальное значение пакета B^c как $k_1^{x1} \bmod m = B^c$. Затем компьютер может, например, выполнить поиск в локальной информационной базе 250 данных значения пакета B, соответствующего значению B^c: в случае несовпадения цифровой паспорт является поддельным и "Джон Доу" (т.е. проверяемый человек, утверждающий, что его зовут Джон Доу) может быть арестован. В случае совпадения B^c с некоторым сохраненным значением пакета B, цифровой паспорт считается подлинным, и сотрудник может выполнить дополнительные проверки безопасности: сотрудник извлекает цифровую фотографию 255 личности, хранящуюся в информационной базе 250 данных, путем отправки запроса через компьютер 290, содержащего серийный номер 235 в A_1, принимает его обратно и отображает принятую фотографию 255 личности на экране компьютера 290: затем сотрудник может визуально сравнить отображаемое лицо (т.е. лицо Джона Доу) с лицом проверяемого человека и оценить, похожи ли эти два лица или нет; и сотрудник извлекает биометрические данные 230e в цифровом 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 одинаковыми, все в порядке, и проверяемый человек действительно является Джоном Доу, владельцем подлинного цифрового биометрического паспорта A_1 (и, таким образом, возможно, также материального биометрического паспорта, из которого получали A_1).

В случае неудачной попытки какой-либо из вышеупомянутых дополнительных проверок безопасности очевидно, что человек перед сотрудником не является истинным владельцем подлинного цифрового биометрического паспорта A_1 и, вероятно, украл паспорт некоего Джона Доу. Таким образом, с помощью защищенного цифрового биометрического 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, т.е. 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 подписи 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 (т.е. 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, т.е. цифровом идентификационном документе AC-ID. Цифровая защитная маркировка 310 (в данном случае в виде двухмерного представления QR-кода) включена в каждый цифровой идентификационный документ компонента самолета, например AC-ID:C_{125}, который связан с соответствующим компонентом самолета, в данном случае C_{125}, установленным на самолете HB-SNO. На фиг. 3, в частности, показан компонент C_{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 идентификационного документа компонента самолета AC-ID:C_{125}, связанного с компонентом C_{125}, со-

держат цифровые данные, соответствующие данным технического паспорта C_{125}: идентификационный код 330a самолета (в данном случае HB-SNO), название 330b изготовителя самолета (в данном случае AeroABC), техническое название 330c компонента (в данном случае лопатка турбины - 1^{oe} кольцо), серийный номер 330d компонента (в данном случае 12781), название 330e изготовителя компонента (в данном случае PCX), дата изготовления компонента 330f (в данном случае 13 ноября 2017 г.), дата сборки компонента на реакторе 330g (в данном случае 24 февраля 2018 г.), имя специалиста, ответственного за выполнение проверки соответствия 330h (в данном случае проверяющий Мартин Вайт) вместе с датой проверки соответствия 330i (в данном случае 20 марта 2018 г.) и (уникальная) цифровая подпись проверяющего 330j (в данном случае 2w9s02u).

Подпись цифрового файла x_{125} цифровых данных D_{125} цифрового файла AC-ID: C_{125} компонента C_{125} вычисляют посредством односторонней хеш-функции H в виде $x_{125} = H(D_{125})$. Таким же образом, все подписи цифровых файлов x_i цифровых данных D_i цифрового файла AC-ID: C_i компонента C_i вычисляют посредством односторонней хеш-функции H в виде $x_i = H(D_j)$ (в данном случае i = 1, ..., μ). Пускай X соответствует всему набору цифровых подписей компонентов $X = (x_1, x_2, ..., x_\mu)$, и пускай X^i соответствует всему набору цифровых подписей компонентов, за исключением подписи x_i, т.е. $X^i = (x_1, x_2, ...* x_{i-1}, x_{i+1}, ..., x_\mu)$. Как уже раскрыто, агрегированную цифровую подпись B для пакета μ цифровых идентификационных документов компонентов самолета AC-ID:C_1, ..., AC-ID:C_μ (цифровых файлов), компонентов самолетов C_1, ..., C_μ, вычисляют посредством одностороннего сумматора f в виде B = f(X). Агрегированную цифровую подпись затем сохраняют в доступной для поиска базе данных (предпочтительно, блокчейн), открытой для специалистов, ответственных за контроль или замену установленных компонентов.

Для заданного цифрового файла AC-ID: C_i пакета соответствующий ключ верификации цифрового файла k_i вычисляют посредством соответствующего частичного одностороннего сумматора в виде $k_i = f(X^i)$. Для каждого компонента C_i, установленного на самолете HB-SNO, связанные цифровые данные D_i и соответствующий ключ верификации k_i встроены в цифровую защитную маркировку, включенную в соответствующий цифровой идентификационный документ компонента самолета AC-ID: C_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 C_{125}, подлежащего контролю, или его ключ верификации k_{125}, считываемый на цифровой защитной маркировке 310 документа 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. Однако в предпочтительном варианте, обеспечивающем полную автономную проверку, компьютер специалиста имеет память, сохраняющую все агрегированные цифровые подписи, относящиеся к самолетам, подлежащим контролю. В данном последнем варианте специалист затем может проверить, является ли компонент подлинным, путем считывания цифровых данных компонента D_{125} на цифровой защитной маркировке 310, проверки совпадения уникального серийного номера 330d (в данном случае 12781), извлеченного из D_{125}, с серийным номером, физически нанесенным на установленный компонент самолета C_{125}, вычисления соответствующей цифровой подписи компонента x_{125} (например, путем запуска запрограммированного приложения на ЦП компьютера, который вычисляет подпись $x_{125} = H(D_{125})$ из считанных цифровых данных D_{125}), вычисления потенциального значения пакета B^c посредством функции одностороннего сумматора, запрограммированной на ЦП компьютера в виде B^c - $k_{125} \otimes x_{125}$ (оператор ⊗, соответствующий одностороннему сумматору f), и проверки совпадения потенциального значения пакета B^c с одним из значений пакета, сохраненных в памяти компьютера (т.е. B, соответствующее пакету цифровых файлов для самолета HB-SNO). В случае полного совпадения (т.е. совпадения серийных номеров и B^c = B), компонент C_{125} считается подлинным и принадлежит к (обновленному) пакету самолета разрешенных компонентов самолета HB-SNO, в случае несовпадения B^c с сохраненным значением пакета B, или в случае несовпадения серийных номеров, компонент C_{125}, вероятно, является подделкой, или является подлинным компонентом, не разрешенным для самолета HB-SNO (например, C_{125} 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 характеристические цифровые данные CDD, относящиеся к соответствующей контрольной уникальной физической характеристике (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, т.е. 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 CDD 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 его компьютера). Затем специалист (или ЦП его компьютера, если он соответствующим образом запрограммирован) сравнивает полученные CDD^c с копией контрольных CDD, сохраненных в памяти компьютера: в случае "обоснованного" совпадения $CDD^c \approx CDD$ (т.е. в пределах некоторого заранее определенного критерия допустимых ошибок) защитная маркировка на основе материала и, следовательно, компонент считаются подлинными.

Как упомянуто выше, копия контрольных физических 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: C компонента C, и может быть получена путем непосредственного считывания на цифровой защитной маркировке. 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 и связанный с ним цифровой идентификационный документ компонента являются подлинными.

В варианте осуществления проверку аутентичности цифрового идентификационного документа компонента и связанного с ним 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 верифицировать аутентичность цифрового идентификационного документа компонента самолета AC-ID: C_{125}, например, относительно оригинального подлинного защищенного цифрового файла. В действительности, если специалист, ответственный за операции контроля (или ремонта), имеет доступ к цифровому файлу AC-ID: C_{125} на своем компьютере (который также 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 ключа верификации k_{125} на цифровой защитной маркировке 310 цифрового идентификационного документа компонента AC-ID: C_{125}; получения контрольного значения B пакета, соответствующего документу AC-ID: C_{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 B; вычисления (с помощью запрограммированной односторонней функции H) подписи цифрового файла x_{125} из считанных цифровых данных компонента D_{125}, с помощью $x_{125} = H(D_{125})$; вычисления потенциального значения пакета (посредством запрограммированного одностороннего сумматора и его соответствующего оператора $\otimes$) B^c с $B^c = k_{125} \otimes x_{125}$; и верификации совпадения потенциального значения пакета B^c с контрольным значением пакета B.

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 содержимому данных оригинального защищенного цифрового файла. Однако настоящее изобретение также совместимо с процессом верификации в режиме "онлайн", например, путем приема (через канал связи) контрольного значения пакета из внешнего источника (например, сервера или блокчейна) или выполнения некоторых или всех этапов вычисления, включающих одностороннюю функцию или односторонний сумматор через внешние вычислительные средства (например, работающие на сервере), или даже выполнения верификации совпадения потенциальной агрегированной цифровой подписи с контрольной агрегированной цифровой подписью (и просто получение результата).

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

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ защиты заданного оригинального цифрового файла из пакета множества оригинальных цифровых файлов (A_1, A_2, A_3) от подделки или фальсификации, при этом каждый оригинальный цифровой файл пакета содержит свои собственные цифровые данные (D_1, D_2, D_3), отличающийся тем, что способ включает этапы

для каждого оригинального цифрового файла пакета, вычисления посредством односторонней функции связанной с цифровым файлом подписи (x_1, x_2, x_3) его цифровых данных;

вычисления контрольной агрегированной цифровой подписи (B), соответствующей пакету оригинальных цифровых файлов, из всех подписей оригинальных цифровых файлов пакета посредством одностороннего сумматора указанных подписей цифровых файлов и предоставления в распоряжение пользователя контрольной агрегированной цифровой подписи;

определения ключа верификации (k_i) цифрового файла, соответствующего подписи указанного заданного оригинального цифрового файла, посредством одностороннего сумматора всех других подписей цифровых файлов, используемых для вычисления контрольной агрегированной цифровой подписи, в результате чего потенциальная подпись цифрового файла соответствует подписи оригинального цифрового файла пакета, в случае вычисления контрольной агрегированной цифровой подписи посредством одностороннего сумматора указанной потенциальной подписи цифрового файла и соответствующего ключа верификации цифрового файла; и

включения в заданный оригинальный цифровой файл цифрового представления машиночитаемой защитной маркировки (110), содержащей представление цифровых данных заданного оригинального цифрового файла и его соответствующего ключа верификации цифрового файла, тем самым получая маркированный оригинальный цифровой файл, цифровые данные которого защищены от подделки или фальсификации.

2. Способ по п.1, отличающийся тем, что контрольная агрегированная цифровая подпись, связанная с пакетом оригинальных цифровых файлов, либо опубликована в среде, открытой для пользователя, либо сохранена в доступной для поиска базе данных агрегированных подписей, открытой для пользователя, либо сохранена в блокчейне (260), либо в базе данных, защищенной блокчейном, открытой для пользователя.

3. Способ по п.2, отличающийся тем, что маркированный оригинальный цифровой файл дополнительно включает данные по доступу к агрегированным подписям, содержащие информацию, достаточную для получения доступа к контрольной агрегированной цифровой подписи, соответствующей пакету оригинальных цифровых файлов, при этом указанная информация представляет собой ссылку в интерфейс сбора агрегированных подписей, соответственно, одного из следующего:

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

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

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

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

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

контрольная агрегированная цифровая подпись, связанная с указанным пакетом оригинальных цифровых файлов, вычислена из всех подписей оригинальных цифровых файлов пакета, включающих подпись виртуального цифрового файла, посредством одностороннего сумматора.

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

6. Способ по любому из пп.1-5, отличающийся тем, что дополнительные цифровые данные, соответствующие цифровым данным, связанным с маркированным оригинальным цифровым файлом, сохранены в доступной для поиска информационной базе (250) данных, открытой для пользователя, посредством интерфейса информационной базы данных, выполненного с возможностью приема от пользователя запроса на информацию, содержащего цифровые данные или соответствующие данные подписи цифрового файла, получаемые из цифрового представления машиночитаемой защитной маркировки маркированного оригинального цифрового файла, и отправки обратно соответствующих дополнительных цифровых данных.

7. Способ по любому из пп.1-6, отличающийся тем, что цифровые данные маркированного оригинального цифрового файла включают контрольные характеристические цифровые данные CDD (230e) соответствующей уникальной физической характеристики связанного объекта или человека.

8. 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 обработки, подключенного к памяти:

сохранения в памяти тестового файла;

считывания представления цифровых данных и ключа верификации тестового файла на цифровом представлении машиночитаемой защитной маркировки в сохраненном тестовом файле и извлечения, соответственно, соответствующих цифровых данных и ключа верификации тестового файла из указанного считанного представления;

сохранения в памяти контрольной агрегированной цифровой подписи соответствующего пакета цифровых файлов и программирования в блоке обработки односторонней функции и одностороннего сумматора;

верификации действительного соответствия извлеченных цифровых данных и ключа верификации тестового файла сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов

вычисления цифровой подписи извлеченных цифровых данных с помощью односторонней функции;

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

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

в результате чего в случае совпадения указанных агрегированных цифровых подписей цифровые данные тестового файла являются данными подлинного оригинального цифрового файла.

9. Способ по п.8, отличающийся тем, что цифровой файл защищен путем сохранения контрольной агрегированной цифровой подписи, связанной с пакетом оригинальных цифровых файлов, в доступной для поиска базе данных агрегированных подписей, 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 базу данных агрегированных подписей и приема обратно контрольной агрегированной цифровой подписи, связанной с пакетом оригинальных цифровых файлов; и

сохранения принятой агрегированной цифровой подписи в памяти.

10. Способ по п.8, отличающийся тем, что цифровой файл защищен согласно способу по п.3, 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

считывания данных по доступу к агрегированным подписям, включенных в тестовый файл;

отправки блоком связи посредством канала связи запроса на агрегированную подпись в указанный интерфейс сбора агрегированных подписей, содержащего цифровые данные или цифровую подпись указанных цифровых данных, получаемые из цифрового представления машиночитаемой защитной маркировки в тестовом файле, и приема обратно соответствующей контрольной агрегированной цифровой подписи связанного пакета; и

сохранения принятой агрегированной цифровой подписи в памяти.

11. Способ по любому из пп.8-10, отличающийся тем, что цифровой файл защищен согласно способу по п.6, и блок обработки дополнительно подключен к средствам связи, выполненным с возможностью отправки в интерфейс информационной базы данных запроса на информацию, содержащего цифровые данные или соответствующую подпись цифрового файла, получаемые из цифрового представления машиночитаемой защитной маркировки в тестовом файле, и приема обратно соответствующих дополнительных цифровых данных.

12. Способ по любому из пп.8-11, отличающийся тем, что цифровой файл защищен согласно способу по п.7, и блок обработки подключен к датчику, выполненному с возможностью обнаружения уникальной физической характеристики связанного объекта или человека, блок обработки запрограммирован для извлечения соответствующих цифровых данных уникальной физической характеристики из сигнала обнаружения, принятого от датчика, блок обработки сохраняет в памяти контрольные характеристические цифровые данные CDD, соответствующие указанной уникальной физической характеристике связанного объекта или человека, при этом способ включает дополнительные этапы, при рассматривании субъекта, представляющего собой, соответственно, указанный связанный объект или человека,

обнаружения уникальной 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, при условии заданного критерия допустимого отклонения, субъект считается подлинным.

13. Маркированный цифровой файл, принадлежащий к пакету множества оригинальных цифровых файлов и защищенный от подделки или фальсификации согласно способу по любому из пп.1-7, при этом каждый оригинальный цифровой файл пакета имеет свои собственные цифровые данные, указанный пакет имеет соответствующую контрольную агрегированную цифровую подпись, при этом файл содержит

цифровое представление машиночитаемой защитной маркировки, включающей представление цифровых данных маркированного цифрового файла и соответствующего ключа верификации цифрового файла.

14. Маркированный цифровой файл по п.13, отличающийся тем, что цифровые данные маркированного цифрового файла включают контрольные характеристические цифровые данные CDD соответствующей уникальной физической характеристики связанного объекта или человека.

15. Маркированный цифровой файл по п.14, отличающийся тем, что уникальная физическая характеристика связанного объекта представляет собой характеристику защитной маркировки на основе материала, нанесенной на связанный объект.

16. Система верификации аутентичности маркированного оригинального цифрового файла, защищенного согласно способу по любому из пп.1-7, или соответствия копии такого цифрового файла относительно оригинального файла, при этом система содержит блок обработки с памятью, память сохраняет контрольную агрегированную цифровую подпись соответствующего пакета цифровых файлов и одностороннюю функцию и односторонний сумматор, запрограммированные в блоке обработки, при этом система выполнена с возможностью

получения тестового файла, представляющего собой указанный цифровой файл или копию цифрового файла, и сохранения полученного тестового файла в памяти;

считывания представления цифровых данных и ключа верификации тестового файла на цифровом представлении машиночитаемой защитной маркировки в сохраненном тестовом файле и извлечения, соответственно, соответствующих цифровых данных и ключа верификации тестового файла из указанного считанного представления;

верификации действительного соответствия извлеченных цифровых данных и ключа верификации тестового файла сохраненной контрольной агрегированной цифровой подписи путем осуществления этапов, запрограммированных в блоке обработки:

вычисления цифровой подписи извлеченных цифровых данных с помощью односторонней функции;

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

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

в результате чего в случае совпадения указанных агрегированных цифровых подписей цифровые данные тестового файла являются данными подлинного оригинального цифрового файла, и система выполнена с возможностью доставки указания того, что цифровые данные на тестовом файле являются данными подлинного оригинального цифрового файла.

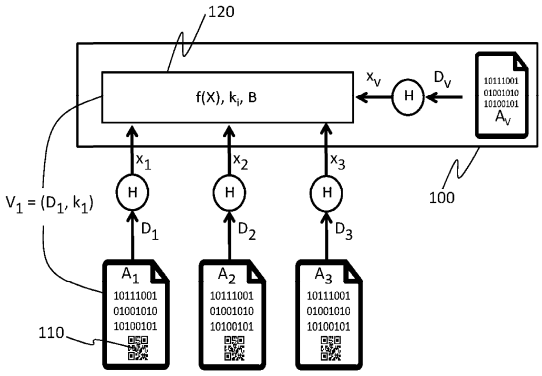
17. Система по п.16 для верификации цифрового файла, защищенного согласно способу по п.7, или соответствия копии такого цифрового файла относительно оригинального файла, дополнительно осна-

щенная 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

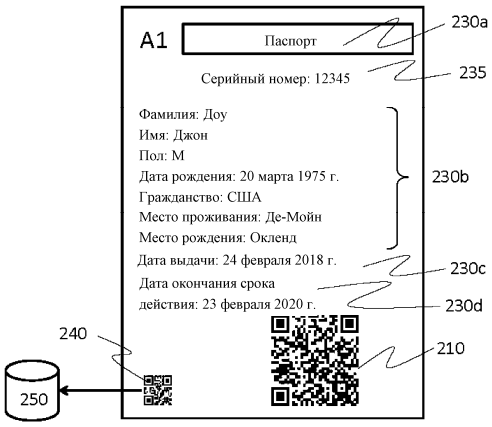
обнаружения с помощью датчика уникальной физической характеристики субъекта, представляющего собой указанный связанный объект или человека, и извлечения соответствующих потенциальных характеристических цифровых данных CDD^c;

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

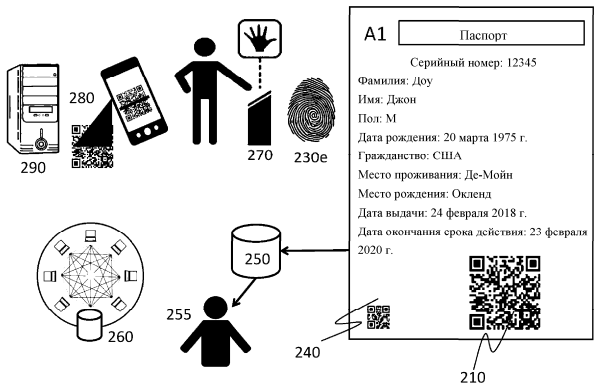
в случае схожести потенциальных характеристических цифровых данных CDD^c с сохраненными контрольными характеристическими цифровыми данными CDD, при условии заданного критерия допустимого отклонения, доставки указания того, что субъект считается подлинным.



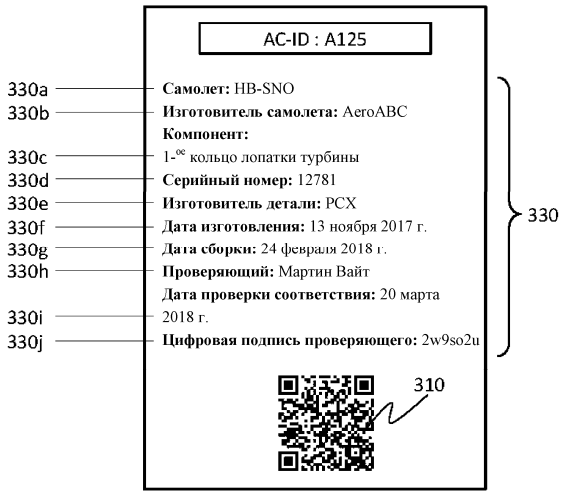
Фиг. 1



Фиг. 2A



Фиг. 2B


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

Фиг. 3