(19) Евразийское патентное ведомство

(21) 202193140 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2022.03.11

(22) Дата подачи заявки
2020.05.28

(51) Int. Cl. ***G07D 7/00*** (2016.01)
G07D 7/12 (2016.01)
G07D 7/20 (2016.01)
G07D 7/0043 (2016.01)
G07D 7/0047 (2016.01)

(54) СЕРТИФИЦИРОВАННЫЙ ТЕКСТОВЫЙ ДОКУМЕНТ

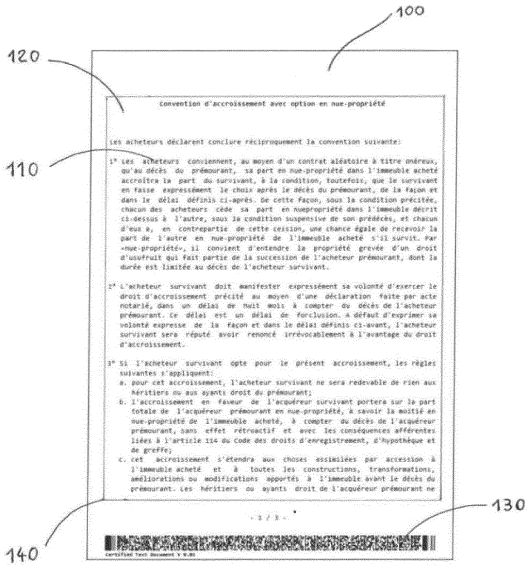
(31) **19177919.8**
(32) **2019.06.03**
(33) **EP**
(86) **PCT/EP2020/064812**
(87) **WO 2020/245024 2020.12.10**

(71) Заявитель:
СИКПА ХОЛДИНГ СА (CH)

(72) Изобретатель:
Деку Эрик (CH)

(74) Представитель:
Рыбина Н.А. (RU)

(57) Настоящее изобретение защищает содержимое цифрового или физического документа от подделки. Оно позволяет автоматически обнаруживать любое изменение в расположении графических символов (например, текст), предоставленных на носителе (например, напечатанных или отображаемых) по отношению к оригинальному расположению путем предоставления на носитель воспроизводимых верифицируемых данных, включающих штрих-код верификации, при одновременном устранении избыточности между данными внутри штрих-кода и графическими символами, и решении проблемы размера штрих-кода, когда размер данных для этих графических символов велик.



202193140 A1

202193140 A1

Первоначально поданное описание

СЕРТИФИЦИРОВАННЫЙ ТЕКСТОВЫЙ ДОКУМЕНТ

Область техники, к которой относится изобретение

Настоящее изобретение относится к области техники способов и систем безопасности и защиты от мошенничества. В частности, настоящее изобретение относится к защите данных от подделки или фальсификации, например, таких как текстовые данные ценного документа (оцифрованного или напечатанного).

Предпосылки создания изобретения

Проблемы подделки и фальсификации цифровых файлов или напечатанных документов являются хорошо известными и серьезными, и их количество постоянно растет. Хорошо известным является пример фальсификации данных, маркированных на оригинальном (цифровом или материальном) документе, таком как документ, удостоверяющий личность, или диплом, и дело обстоит еще хуже, если рассматривать цифровую копию оригинального (возможно, подлинного) цифрового/материального документа. Простое отслеживание идентификаторов, таких как серийные номера, или даже включение некоторых цифровых водяных знаков, как правило, является слабым решением, поскольку фальсификаторы могут легко скопировать такие номера или цифровые водяные знаки.

Существует множество известных методов защиты содержимого цифрового или физического документа от подделки. Например, взяв хеш-значение цифровых данных из оригинального цифрового документа или из оцифрованной версии оригинального физического документа (например, путем сканирования документа и извлечения текстовых данных с помощью программного обеспечения сканера OCR) и сохранения хеш-значения в реестре (например, простая база данных или блокчейн). Затем путем сканирования содержимого

данных исследуемого документа, визуально представленного на физическом носителе (например, носитель может быть листом бумаги, на котором напечатаны данные), и вычисления хеш-значения указанного содержимого данных, а затем сравнения вычисленного хеш-значения с хеш-значением, сохраненным в реестре, соответствующем оригинальному документу, можно обнаружить изменение содержимого данных. Однако, недостатком этого способа является то, что из-за некоторого изменения визуального представления на носителе содержимого документа, даже если этот документ является подлинным, вычисленное хеш-значение может отличаться от сохраненного хеш-значения. Это различие также может быть связано со способом выполнения операции сканирования или даже зависеть от типа используемого сканера (два разных сканера могут дать два противоположных результата). Это также верно для цифрового документа, отображаемого на носителе, таком как экран (например, компьютера): даже если содержимое документа является подлинным, любое изменение отображаемого содержимого будет генерировать, при сканировании отображаемого содержимого для верификации, хеш-значение, отличное от сохраненного хеш-значения. Таким образом, на практике сканирование документа и вычисление хеш-значения захваченного изображения не работают, потому что каждый раз при сканировании документа обычно получается другое хеш-значение. Использование сканера OCR («Оптическое распознавание символов») перед вычислением хеш-значения не решает вышеупомянутую проблему, поскольку не существует системы OCR, которая работает на 100%: например, если просто точка становится запятой, или буква «l» (т. е. L) становится «1» (то есть единицей), вычисленное хеш-значение будет другим.

Некоторые существующие методы защиты бумажных документов (например, сертификатов, дипломов, контрактов и т. д.) с использованием лишь небольшого объема информации, извлеченной из документа, включают создание двухмерного штрих-кода (например, QR-кода), размещение извлеченной информации внутри двухмерного штрих-кода и его печать на документе. Каждый раз при считывании двухмерного штрих-кода получается один и тот же

результат, но с недостатком, заключающимся в том, что информацию, включенную в штрих-код, необходимо сравнивать с информацией, напечатанной на документе. Более того, если кто-то хочет защитить, например, полнотекстовую страницу, необходимо поместить полный текст в штрих-код, и, таким образом, штрих-код становится огромным по размеру и требует много места на странице, что воспринимается читателем как что-то нарушающее обычный порядок (так что на практике полный текст, который может быть закодирован, имеет ограниченный размер), и становится необходимым (и утомительным) сравнивать несколько тысяч символов между напечатанным текстом и текстом, декодированным с помощью штрих-кода.

Краткое описание изобретения

Настоящее изобретение направлено на устранение вышеупомянутых недостатков предшествующего уровня техники, касающихся подделки и фальсификации цифровых файлов или напечатанных документов, путем обеспечения автоматического обнаружения любого изменения в расположении маркированных (соответственно отображаемых) графических символов (например, текста) в отношении к оригинальному расположению, и, в частности, устранение избыточности между данными внутри кода и напечатанным (соответственно отображаемым) текстом, избегая бремени визуального сравнения текста внутри кода с напечатанным (или отображаемым) текстом, одновременно решая проблему слишком большого размера кода, когда размер данных для напечатанного (или отображаемого) текста велик.

Таким образом, настоящее изобретение направлено на обеспечение точного и надежного способа получения на материальном носителе, таком как дисплей (например, экран компьютера) или подложка (например, лист бумаги, этикетка, упаковка), видимых графических символов (например, текстовых символов или глиф), соответствие которых аутентичным эталонным графическим символам пользователь может легко проверить, считывая указанные видимые графические символы, и это позволяет устранить недостатки предшествующего уровня

техники. Графические символы являются удобочитаемыми для человека и взяты из заданного конечного набора графических символов (например, таких как текстовые символы из алфавита). Таким образом, пользователь может верифицировать удобочитаемые для человека графические символы, отображаемые или маркированные на подложке согласно настоящему изобретению, и любая попытка изменить любую часть графических символов может быть обнаружена.

Таким образом, настоящее изобретение относится к «способу нанесения маркировки», т. е. способу генерирования на носителе верифицируемых графических данных с использованием заданного конечного набора графических символов, причем носитель является дисплеем или подложкой, включающему этапы:

- сохранения в памяти блока обработки блока графических данных, содержащего цифровое представление графических символов;

- обработки блоком обработки цифрового представления графических символов сохраненного блока графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки, для генерирования данных с исправлением ошибок в соответствующем блоке данных с исправлением ошибок;

- форматирования блока графических данных и блока данных с исправлением ошибок блоком обработки для предоставления, соответственно, в блоке удобочитаемых для человека графических данных удобочитаемого для человека представления графических символов блока графических данных и в блоке машиночитаемых данных с исправлением ошибок машиночитаемого представления данных с исправлением ошибок блока данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов блока графических данных для получения соответствующего блока верифицируемых графических данных, содержащего указанный блок

удобочитаемых для человека графических данных и указанный блок машиночитаемых данных с исправлением ошибок; и

(i) отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок полученного блока верифицируемых графических данных на дисплее, подключенном к блоку обработки, или

(ii) нанесения маркировки на подложку устройством для нанесения маркировки, подключенным к блоку обработки и оснащенным блоком контроля, выполненным с возможностью контроля операции нанесения маркировки на основании данных, принятых от блока обработки, в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок блока верифицируемых графических данных, принятого от блока обработки,

с предоставлением тем самым на носителе удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые верифицируются пользователем.

Машиночитаемое представление данных с исправлением ошибок может быть любым из буквенно-цифрового представления или представления в виде штрих-кода (одномерный штрих-код, или двухмерный штрих-код, такой как, например, код DataMatrix или QR-код). Предпочтительно, штрих-код может быть обычным линейным штрих-кодом PDF417, который можно считывать простым линейным сканером, проводимым по штрих-коду. Предпочтительно, графические символы могут быть текстовыми символами, а конечный набор графических символов - алфавитом. Предпочтительно, устройство для нанесения маркировки может быть принтером (например, струйным принтером), а подложка может быть листом бумаги или этикеткой. Также предпочтительно, чтобы код с исправлением ошибок мог быть кодом с исправлением ошибок Рида-Соломона.

В первом варианте вышеупомянутый способ нанесения маркировки может включать дополнительные этапы:

- вычисления с помощью хеш-функции, запрограммированной в блоке обработки, хеш-значения блока графических данных, или блока данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока графических данных и блока данных с исправлением ошибок; и

- сохранения вычисленного хеш-значения как эталонного хеш-значения в реестре.

Хеш-функция является хорошо известным примером односторонней функции, т. е. функции, которую легко вычислить, но трудно инвертировать(см., например, S. Goldwasser and M. Bellare “Lecture Notes on Cryptography”, MIT, июль 2008 г., http://www-cse.ucsd.edu/users/mihir). Предпочтительно, криптографическая хеш-функция может принадлежать семейству SHA-2, как, SHA-256, например, задавая хеш-значения размером 256 битов: данная функция практически необратима и устойчива к коллизиям, то есть вероятность того, что две разные группы входных данных приведут к одним и тем же выходным данным, ничтожна. Также предпочтительно, чтобы реестр мог представлять собой блокчейн, который преимущественно обеспечивает неизменяемую запись данных. Необязательно, может быть дополнительный этап подписывания вычисленного эталонного хеш-значения с помощью личного ключа подписи блоком обработки для получения соответствующего подписанного эталонного хеш-значения и сохранения или дальнейшего предоставления на носителе подписанного эталонного хеш-значения. С помощью этой альтернативы пользователь, имеющий открытый ключ, соответствующий личному ключу, может проверить, что подписанное эталонное хеш-значение, считанное на носителе, является подлинным, поскольку оно подписано правильным личным ключом.

Во втором варианте вышеупомянутого способа нанесения маркировки носитель содержит множество частей, и блок верифицируемых графических данных разделяют на одинаковое множество субблоков верифицируемых графических данных, и соответствующие удобочитаемые для человека графические символы и машиночитаемое представление данных с исправлением ошибок, соответственно, распределяют вместе на соответствующие части носителя, посредством следующих этапов, на которых:

- блок графических данных разделяют на множество субблоков графических данных, и каждый субблок графических данных форматируют для предоставления удобочитаемого для человека представления его графических символов в соответствующем субблоке удобочитаемых для человека графических данных;

- для каждого субблока графических данных цифровое представление его графических символов извлекают и обрабатывают с помощью кода с исправлением ошибок для генерирования соответствующих данных с исправлением ошибок в субблоке данных с исправлением ошибок;

- каждый субблок данных с исправлением ошибок форматируют для предоставления в соответствующем субблоке машиночитаемых данных с исправлением ошибок машиночитаемого представления соответствующих данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов соответствующего субблока удобочитаемых для человека графических данных для получения соответствующего субблока верифицируемых графических данных, содержащего указанный субблок удобочитаемых для человека графических данных и указанный субблок машиночитаемых данных с исправлением ошибок; и

- на этапе (i), отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением

ошибок каждого полученного субблока верифицируемых графических данных на дисплее, или

- на этапе (ii), нанесения маркировки на подложку устройством для нанесения маркировки в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок каждого субблока верифицируемых графических данных, принятого блоком контроля от блока обработки,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые верифицируются пользователем.

Данный второй вариант способа нанесения маркировки для генерирования верифицируемых графических символов на носителе особенно адаптирован в случае документа, состоящего из нескольких страниц текста (т. е. носитель имеет множество частей): полный текст разделяют на множество частей, причем каждая часть текста соответствует странице текста и, таким образом, каждая страница документа, предусмотренная на носителе, содержит удобочитаемое для человека представление графических символов соответствующего субблока графических данных вместе с отдельным машиночитаемым представлением данных с исправлением ошибок соответствующего субблока данных с исправлением ошибок (например, в виде штрих-кода PDF417, показанного на фиг. 1).

С целью обеспечения возможности пользователю дополнительного определения того, являются ли удобочитаемые для человека графические символы и соответствующий субблок машиночитаемых данных с исправлением ошибок, считанный на носителе (т. е. на части носителя, соответствующей субблоку графических данных блока графических данных) аутентичными или нет, вышеупомянутый второй вариант осуществления способа нанесения маркировки

может дополнительно включать признаки одного из следующих двух подвариантов.

Согласно первому подварианту второго варианта способа нанесения маркировки,

- хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

- для каждого хеш-значения субблока вычисляют соответствующее машиночитаемое представление указанного хеш-значения субблока;

- одновременно с каждым субблоком верифицируемых графических данных, соответствующее машиночитаемое представление хеш-значения субблока дополнительно предоставляют на соответствующей части носителя;

- эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как конкатенацию всех вычисленных хеш-значений субблоков; и

- эталонное агрегированное хеш-значение сохраняют в реестре,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

Согласно второму подварианту второго варианта способа нанесения маркировки,

- хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических

данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

- эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как значение корневого узла дерева, имеющего вычисленные хеш-значения субблоков как значения листовых узлов, причем дерево содержит узлы, расположенные согласно заданной упорядоченности узлов в дереве, указанное дерево содержит уровни узлов, начиная от листовых узлов до корневого узла, причем каждое значение узла, отличного от листового, дерева соответствует хеш-значению конкатенации соответственных значений узлов его дочерних узлов согласно упорядоченности конкатенации дерева, значение корневого узла соответствует хеш-значению конкатенации значений узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

- для каждого хеш-значения субблока связанный ключ пути верификации субблока определяют как ряд хеш-значений выбранных узлов, отличных от листовых, дерева, необходимых для извлечения значения корневого узла из указанного хеш-значения субблока;

- машиночитаемое представление каждого ключа пути верификации субблока включают, одновременно с соответственно соответствующим субблоком графических данных и субблоком данных с исправлением ошибок, в субблок верифицируемых графических данных, причем субблок верифицируемых графических данных дополнительно форматируют для предоставления машиночитаемого представления указанного ключа пути верификации субблока отдельно от удобочитаемого для человека представления связанного субблока графических данных и машиночитаемого представления связанного субблока данных с исправлением ошибок; и

(iii) эталонное агрегированное хеш-значение сохраняют в реестре, или

(iv) эталонное агрегированное хеш-значение предоставляют в распоряжение пользователя,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

Настоящее изобретение также относится к «способу верификации», соответствующему вышеупомянутому «способу нанесения маркировки», т. е. способу верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемым представлением данных с исправлением ошибок на носителе, которые были сгенерированы согласно вышеупомянутому способу генерирования верифицируемых графических символов на указанном носителе, включающему этапы:

- сканирования сканером, оснащенным блоком формирования изображения, блоком обработки сканера, имеющим память сканера и подключенным к дисплею сканера, удобочитаемых для человека графических символов на носителе для получения путем обработки изображения сканированных удобочитаемых для человека графических символов блока сканированных графических данных, представляющего собой цифровое представление указанных сканированных удобочитаемых для человека графических символов;

- сканирования сканером машиночитаемого представления данных с исправлением ошибок на носителе для получения с помощью машиночитаемого декодера, запрограммированного в блоке обработки сканера, соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок, причем блок сканированных данных с исправлением ошибок представляет собой цифровое представление указанных сканированных данных с исправлением ошибок;

- исправления блока сканированных графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки сканера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как соответствующих исправленных удобочитаемых для человека графических символов на дисплее сканера, или

(b) указания сканером того, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти сканера.

Таким образом, согласно настоящему изобретению пользователь может непосредственно визуализировать на дисплее сканера (альтернатива (a)) оригинальные графические символы (например, оригинальный текст документа) благодаря исправлению сканированного текста, а затем легко сравнивать отображаемые графические символы (т. е. исправленные удобочитаемые для человека графические символы) с графическими символами на носителе и обнаруживать любые изменение или мошенничество.

Сканер может быть специально предназначенным устройством или может быть простым смартфоном, оснащенным камерой и имеющим запрограммированное приложение, выполненное с возможностью запуска в процессоре указанного смартфона и выполнения этапов вышеупомянутого способа верификации графических символов и соответствующих машиночитаемых данных с исправлением ошибок, предоставленных на носителе. Некоторые этапы способа верификации можно также выполнять на удаленном сервере, связанном со сканером: например, сканер может отправлять блок сканированных графических данных и машиночитаемые данные с исправлением ошибок на сервер,

подходящим образом запрограммированные средства обработки сервера могут затем выполнять этапы получения соответствующих сканированных данных с исправлением ошибок, исправления блока сканированных графических данных (с помощью кода с исправлением ошибок, запрограммированного в сервере) с использованием сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных и отправки блока исправленных сканированных графических данных в сканер (возможно с сообщением того, содержит ли блок сканированных графических данных ошибку, или сохранением данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, на сервере).

Первый вариант вышеупомянутого способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно первому варианту способа нанесения маркировки, причем хеш-функция запрограммирована в блоке обработки сканера, и сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включает дополнительные этапы:

- вычисления согласно первому варианту способа нанесения маркировки с помощью хеш-функции, запрограммированной в блоке обработки сканера, хеш-значения сканирования блока исправленных сканированных графических данных, или блока сканированных данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока исправленных сканированных графических данных и блока сканированных данных с исправлением ошибок;

- получения эталонного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное хеш-значение с хеш-значением сканирования; и

(e) указания результата операции проверки, или

(f) сохранения результата операции проверки в памяти сканера.

Таким образом, даже при изменении одного бита данных в данных, оригинально предоставленных на носителе, хеш-значение сканирования будет сильно отличаться от эталонного хеш-значения, и изменение будет обнаружено.

Во втором варианте вышеупомянутого способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно второму варианту способа нанесения маркировки,

- операция сканирования удобочитаемых для человека графических символов на носителе включает сканирование графических символов соответствующего субблока графических данных для получения путем обработки изображения соответствующего субблока сканированных графических данных как цифрового представления сканированных графических символов субблока;

- операция сканирования машиночитаемых данных с исправлением ошибок на носителе включает сканирование данных с исправлением ошибок соответствующего субблока данных с исправлением ошибок для получения соответствующего субблока сканированных данных с исправлением ошибок;

- операция исправления блока сканированных графических данных включает исправление графических данных субблока сканированных графических данных с использованием соответствующего субблока сканированных данных с исправлением ошибок для получения соответствующего субблока исправленных сканированных графических данных; и

- операция (a) отображения визуального представления блока исправленных сканированных данных включает отображение визуального представления субблока исправленных сканированных графических данных;

- операция (b) указания того, содержит ли блок сканированных графических данных ошибку, включает указание того, содержит ли субблок сканированных графических данных ошибку;

- операция (c) сохранения данных результата сканирования включает сохранение того, содержит ли субблок сканированных графических данных ошибку.

Первый подвариант второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно первому подварианту второго варианта способа нанесения маркировки, хеш-функция и код с исправлением ошибок запрограммированы в блоке обработки сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления хеш-значения субблока на носителе блоком обработки сканера, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включает дополнительные этапы:

- вычисления для каждой части носителя с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования соответствующего субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока исправленных сканированных графических данных и указанного субблока сканированных данных с исправлением ошибок;

- в случае если невозможно вычислить хеш-значение субблока сканирования для части носителя, сканирования и декодирования машиночитаемого представления хеш-значения субблока на указанной части носителя для получения соответствующего декодированного хеш-значения субблока, а также

использования этого декодированного хеш-значения субблока как хеш-значения субблока сканирования для этой части носителя;

- вычисления агрегированного хеш-значения сканирования как конкатенации всех хеш-значений субблока сканирования;

- получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

- указания результата операции проверки сканером.

Данный первый подвариант второго варианта способа нанесения маркировки позволяет проверять аутентичность графических символов всех считываемых частей носителя, даже если некоторая(-ые) часть(-и) является(являются) несчитываемой(-ыми) (например, благодаря сильному изменению графических символов и/или данных с исправлением ошибок, предоставленных на указанной(-ых) части(-ях)), путем извлечения исправленного агрегированного хеш-значения. Действительно, если хеш-значение субблока сканирования нельзя вычислить для определенной части носителя, его все еще можно получить путем считывания и декодирования машиночитаемого представления хеш-значения субблока на указанной части носителя, и использовать декодированное хеш-значение в конкатенации всех хеш-значений для определения потенциального агрегированного хеш-значения, подлежащего сравнению с эталонным агрегированным хеш-значением.

Второй подвариант второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, эталонное агрегированное хеш-значение сохранено в реестре, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал

связи с реестром, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включает дополнительные этапы:

- вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

- сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

- вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

- получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

- указания результата операции проверки сканером.

Данный второй подвариант второго варианта способа верификации позволяет независимо проверять аутентичность каждой страницы документа, поскольку

потенциальное хеш-значение корневого узла можно вычислить из данных, считываемых на каждой странице, и сравнить с эталонным агрегированным хеш-значением.

Третий подвариант второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, эталонное агрегированное хеш-значение, предоставленное в распоряжение пользователя, сохранено в памяти сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включает дополнительные этапы:

- вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

- сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

- сканирования на носителе эталонного агрегированного хеш-значения для получения сканированного эталонного агрегированного хеш-значения;

- вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

- проверки того, совпадает ли эталонное агрегированное хеш-значение, сохраненное в памяти сканера, с агрегированным хеш-значением сканирования; и

- указания результата операции проверки сканером.

Данный третий подвариант второго варианта способа верификации позволяет независимо автономно проверять аутентичность каждой страницы документа, поскольку потенциальное хеш-значение корневого узла можно вычислить из данных, считываемых на каждой странице, и сравнить с эталонным агрегированным хеш-значением, сохраненным в памяти сканера.

Настоящее изобретение также относится к альтернативному способу верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее компьютера, которые были сгенерированы согласно вышеупомянутому способу генерирования верифицируемых графических символов на указанном дисплее, в котором компьютер имеет приложение для сканирования, запрограммированное в процессоре, выполненном с возможностью сканирования отображаемых удобочитаемых для человека графических символов и машиночитаемых данных с исправлением ошибок, включающему этапы:

- сканирования отображаемых удобочитаемых для человека графических символов с помощью приложения для сканирования, запущенного в процессоре компьютера, для получения блока сканированных графических данных, представляющего собой цифровое представление сканированных удобочитаемых для человека графических символов;

- сканирования отображаемых машиночитаемых данных с исправлением ошибок и с помощью машиночитаемого декодера приложения для сканирования, запущенного в процессоре компьютера, декодирования сканированных машиночитаемых данных с исправлением ошибок для получения соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок;

- исправления блока сканированных графических данных с помощью кода с исправлением ошибок приложения для сканирования, запущенного в процессоре компьютера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как исправленных удобочитаемых для человека графических символов на дисплее, или

(b) отображения сообщения, указывающего на то, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти компьютера.

Данный альтернативный способ верификации (как «способ верификации отображаемых данных») особенно адаптирован для поддержки возможностей офисного программного обеспечения (например, приложений для обработки текста) по обнаружению мошенничества или ошибок в текстовых документах (например, контрактах, отчетах и т. д.), отображаемых на экране компьютера, которые были сгенерированы на компьютере или загружены в компьютер (например, из внешней памяти, такой как USB-ключ, или через канал связи с внешним сервером, например, с почтовым сервером). Определенное приложение, запущенное на компьютере, фактически выполняет операции, осуществляемые сканером в способе верификации.

Настоящее изобретение дополнительно относится к носителю, маркированному удобочитаемыми для человека графическими символами и машиночитаемым представлением связанных данных с исправлением ошибок согласно вышеупомянутому способу нанесения маркировки, или любому из его первого и второго вариантов, или любому из его первого и второго подвариантов указанного второго варианта. Указанный носитель дополнительно маркирован:

- машиночитаемым представлением хеш-значения субблока согласно первому подварианту второго варианта способа нанесения маркировки, или

- связанным машиночитаемым представлением ключа пути верификации согласно второму подварианту второго варианта способа нанесения маркировки.

Согласно другому аспекту настоящее изобретение относится к сканеру, оснащенному блоком формирования изображения, блоком обработки сканера и дисплеем сканера, при этом блок обработки сканера запрограммирован на запуск сканера, выполненного с возможностью считывания верифицируемых графических данных, маркированных на носителе согласно настоящему изобретению, путем реализации этапов способа верификации, или его второго варианта и третьего подварианта его второго варианта.

Сканер может дополнительно быть оснащен блоком связи сканера, выполненным с возможностью установления связи через канал связи с реестром, при этом блок обработки сканера дополнительно запрограммирован на запуск сканера, выполненного с возможностью получения хеш-значения из реестра, путем реализации этапов способа согласно любому из первого варианта способа верификации или первого подварианта или второго подварианта второго варианта способа верификации.

Наконец, настоящее изобретение также относится к компьютерному программному продукту, выполненному с возможностью, при запуске на компьютере, оснащенном процессором, памятью и дисплеем, реализации этапов альтернативного способа верификации (т. е. указанного «способа верификации

отображаемых данных») для верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее, которые были сгенерированы согласно способу нанесения маркировки.

Далее настоящее изобретение будет описано более полно со ссылкой на прилагаемые чертежи, на которых одинаковые цифры представляют одинаковые элементы на разных фигурах и на которых проиллюстрированы основные аспекты и признаки настоящего изобретения.

Краткое описание чертежей

На **фиг. 1** проиллюстрирован пример носителя, маркированного верифицируемыми графическими символами согласно способу нанесения маркировки настоящего изобретения.

На **фиг. 2** представлена блок-схема, на которой проиллюстрирован процесс генерирования и нанесения маркировки в виде верифицируемых графических символов на подложке согласно способу нанесения маркировки настоящего изобретения.

На **фиг. 3** представлена блок-схема процесса генерирования и отображения верифицируемых графических символов на дисплее согласно способу нанесения маркировки настоящего изобретения.

На **фиг. 4** представлена блок-схема, на которой проиллюстрирован процесс генерирования и предоставления верифицируемых графических символов на носителе согласно второму варианту способа нанесения маркировки настоящего изобретения.

На **фиг. 5** показан пример хеш-дерева, используемого во втором подварианте второго варианта способа нанесения маркировки согласно настоящему изобретению.

На **фиг. 6** представлена блок-схема, на которой проиллюстрирован процесс верификации графических символов и машиночитаемых данных, предоставленных на носителе согласно способу верификации настоящего изобретения.

На **фиг. 7** представлена блок-схема, на которой проиллюстрирован вариант осуществления второго варианта способа верификации согласно настоящему изобретению.

Подробное описание

На фиг. 1 проиллюстрирован пример носителя 100, представляющего собой подложку (в данном случае лист бумаги), маркированную удобочитаемым для человека представлением графических символов 110 (в данном случае буквы алфавита, знаки пунктуации и числа, напечатанные на листе 100 бумаги), представляющих собой фрагмент текста контракта, напечатанный в текстовой области 120 носителя 100, вместе с машиночитаемым двухмерным штрих-кодом 130 (в данном случае штрих-код PDF417, т. е. штрих-код «Portable Data File» 417), напечатанный под текстовой областью 120. Фрагмент текста в текстовой области 120 является удобочитаемым для человека представлением соответствующего блока графических данных графических символов.

Двухмерный штрих-код обычно содержит следующие части:

- рисунок локализации (например, форма «L» и линия синхронизации для DataMatrix, или три больших квадрата для QR-кода);

- некоторые информационные поля о формате кода;

- зону данных для хранения данных; а также

- машиночитаемые данные с исправлением ошибок для исправления ошибок считывания (например, данные с исправлением ошибок Рида-Соломона).

Код с исправлением ошибок обычно использует таблицу соответствия, т. е. преобразование между графическими символами заданного конечного набора эталонных графических символов (например, глифов, таких как читаемые символы алфавита) и взаимно однозначными соответствующими кодами (например, символами, закодированными на заданное число m битов).

Штрих-код 130 PDF417 – это хорошо известный многослойный линейный штрих-код (стандарт ISO 15438), который можно считывать с помощью простого линейного сканирования, проводимого по штрих-коду. В варианте осуществления, показанном на фиг. 1, штрих-код 130 PDF417 представляет собой машиночитаемое представление блока данных с исправлением ошибок, который был получен путем применения кода с исправлением ошибок (в данном случае, обычного кода Рида-Соломона) к блоку графических данных расположения графических символов, соответствующих фрагменту текста, показанному в текстовой области 120. Штрих-код 130 PDF417 также содержит (как обычно) данные, относящиеся к версии кода (Рида-Соломона), используемого для вычисления данных с исправлением ошибок, данные, относящиеся к шрифтам, размеру шрифта и межстрочному интервалу текста, числу строк и столбцов текста, относительному местоположению текстовой области относительно маркеров 140, ограничивающих границы блока графических данных (в данном случае, простые метки, указывающие на углы прямоугольной текстовой области 120). Необязательно, штрих-код 130 может дополнительно содержать данные подписи. Эти данные подписи могут быть, например, подписью цифрового представления фрагмента текста с помощью личного ключа шифрования (эта подпись может быть дешифрована с помощью соответствующего открытого ключа).

Фрагмент текста, напечатанный в текстовой области 120, и напечатанный штрих-код 130 PDF417, соответственно, являются примерами удобочитаемых для человека графических символов HrGS и машиночитаемого представления соответствующих данных с исправлением ошибок MrECD, которые были получены посредством способа нанесения маркировки, проиллюстрированного

на фиг. 2. Действительно, на фиг. 2 показана блок-схема процесса генерирования верифицируемых графических данных VGD на подложке (в данном случае листе бумаги) с помощью блока обработки (CPU), который вычисляет блок верифицируемых графических данных VGDB, и нанесения маркировки на подложку с помощью устройства для нанесения маркировки (например, струйного принтера), получившего указанный блок верифицируемых графических данных VGDB. Блок графических данных GDB 210, содержащий цифровое представление графических символов DGS, сохраняют в памяти CPU, при этом каждый графический символ принадлежит заданному конечному набору из M ($M \geq 1$) графических символов {GS(1),…, GS(M)}. Например, конечный набор из M = 26 букв от A до Z английского алфавита. Каждый графический символ GS(i), $i \in \{1,\ldots, M\}$, имеет свое соответствующее цифровое представление DGS(i), и цифровое представление графических символов DGS блока графических данных GDB содержит столько DGS(i), сколько графических символов во фрагменте текста (например, фрагменте текста в текстовой области 120). Процесс генерирования начинается 200 с извлечения 220 цифрового представления графических символов DGS из сохраненного блока графических данных GDB и обработки с помощью запрограммированного кода с исправлением ошибок ECC извлеченного цифрового представления графических символов DGS для получения соответствующих данных с исправлением ошибок ECD. Эти данные с исправлением ошибок ECD представлены в блоке данных с исправлением ошибок ECDB 230. Полученный блок данных с исправлением ошибок ECDB затем форматируют 240 для предоставления соответствующих машиночитаемых данных с исправлением ошибок MrECD, представленных в блоке машиночитаемых данных с исправлением ошибок MrECDB. Блок графических данных GDB также форматируют для получения 215 соответствующего удобочитаемого для человека представления его графических символов HrGS, которые включают в блок данных удобочитаемого для человека графического представления HrGDB. В результате получают 250 блок верифицируемых графических данных VGDB, который состоит из двух соответственных блоков данных: блока данных удобочитаемого для человека

графического представления HrGDB и блока машиночитаемых данных с исправлением ошибок MrECDB. Символически: VGDB = HrGDB + MrECDB. Полученный блок верифицируемых графических данных VGDB затем отправляют на устройство для нанесения маркировки, в данном случае принтер, и их содержимое наносят в виде маркировки 260 (т. е. печатают) на подложку 100 согласно форматированию как соответствующие верифицируемые графические данные VGD. Нанесенные в виде маркировки VGD содержат соответствующие удобочитаемые для человека графические символы HrGS и машиночитаемые данные с исправлением ошибок MrECD (символически: VGD = HrGS + MrECD), которые, соответственно, помещают на лист 100 бумаги согласно форматированию (т. е. как отдельные блоки данных), что говорит о завершении 270 процесса генерирования верифицируемых графических данных на подложке 100 (см. этап (ii) вышеупомянутого способа нанесения маркировки).

Вместо нанесения маркировки на подложку можно отображать фрагмент текста, например, на дисплее планшета или компьютера, как проиллюстрировано на блок-схеме на фиг. 3. Как и на предыдущей фиг. 2, блок графических данных GDB 310, содержащий цифровое представление графических символов DGS, сохраняют в памяти CPU (каждый графический символ принадлежит к заданному конечному набору из $M \geq 1$ графических символов {GS(1),…, GS(M)}). Блок графических данных GDB содержит столько цифровых представлений DGS(i), сколько графических символов GS(i) в отображаемом фрагменте текста. Процесс генерирования начинается 300 с извлечения 320 цифрового представления графических символов DGS из сохраненного блока графических данных GDB и обработки с помощью запрограммированного кода с исправлением ошибок ECC извлеченных DGS для получения соответствующих данных с исправлением ошибок ECD. Эти данные с исправлением ошибок ECD включают в блок данных с исправлением ошибок ECDB 330, который затем форматируют 340 для предоставления соответствующих машиночитаемых данных с исправлением ошибок MrECD, включенных в блок машиночитаемых данных с исправлением ошибок MrECDB. Блок графических данных GDB также

форматируют для получения 315 соответствующего удобочитаемого для человека представления его графических символов HrGS, которые включают в блок данных удобочитаемого для человека графического представления HrGDB. В результате получают 350 блок верифицируемых графических данных VGDB, состоящий из двух соответственных блоков данных HrGDB и MrECDB (символически, VGDB = HrGDB + MrECDB). Блок верифицируемых графических данных VGDB затем отображают 360 на дисплее согласно форматированию как отдельные удобочитаемое для человека представление графических символов HrGS и машиночитаемое представление данных с исправлением ошибок MrECD, что говорит о завершении 370 процесса генерирования верифицируемых графических символов на носителе (см. этап (i) вышеупомянутого способа нанесения маркировки).

Согласно настоящему изобретению несколько вариантов и подвариантов способа нанесения маркировки повышают уровень доверия в соответствии между удобочитаемыми для человека графическими символами, непосредственно считываемыми на носителе пользователем, и удобочитаемой для человека версией, которую можно извлечь из машиночитаемого представления данных с исправлением ошибок (считываемого предназначенным устройством). Эти варианты соответствуют вышеупомянутым первому и второму вариантам.

Первый вариант способа нанесения маркировки использует квази-необратимость односторонних функций, таких как, например, хеш-функции. В этом первом варианте, после осуществления этапов вышеупомянутого способа нанесения маркировки, хеш-функцию H, запрограммированную в блоке обработки, дополнительно используют для получения хеш-значения цифрового представления графических символов или данных с исправлением ошибок (или некоторых частей этих данных), путем вычисления хеш-значения блока графических данных GDB, или блока данных с исправлением ошибок ECDB, или любой части конкатенации (GDB $\oplus$ ECDB) блока графических данных GDB и блока данных с исправлением ошибок ECDB. Хеш-значение (например, с

помощью хеш-функции SHA-256) можно вычислить на основании простого блока графических данных: H(GDB). Предпочтительно, хеш-значение вычисляют на основании блока полной конкатенации: H(GDB ⊕ ECDB). В случае вычисления хеш-значения только на основании части конкатенации блока графических данных GDB и блока данных с исправлением ошибок ECDB, очевидно, что длина в битах этой части должна быть достаточной для обеспечения хорошего уровня безопасности, например, должна по меньшей мере быть равной 100 битам и предпочтительно иметь длину в битах результата, предоставленного выбранной хеш-функцией: например, с помощью хеш-значения SHA-256 длина части в битах составляет по меньшей мере 256 битов (тогда на практике хеш-значение является необратимым). Таким образом, любое изменение, даже одного бита, в аргументе хеш-функции (т. е. любое изменение графических символов или машиночитаемых данных на носителе) приведет к генерированию другого хеш-значения.

В указанном первом варианте способа нанесения маркировки хеш-значение дополнительно сохраняют в реестре, предпочтительно блокчейне (тогда сохраненное значение является практически неизменным), как эталонное хеш-значение H_{ref}. Необязательно, эталонное хеш-значение H_{ref} можно дополнительно подписывать с помощью ключа шифрования, предпочтительно личного ключа Pr_k (сохраненного в памяти блока обработки), для получения соответствующего подписанного эталонного хеш-значения $S(H_{ref})$, и подписанное эталонное хеш-значение $S(H_{ref})$ сохраняют (например, в реестре, таком как база данных или блокчейн) или предоставляют на носителе, эта последняя альтернатива совместима с автономным процессом верификации, при условии что открытый ключ Pu_k, соответствующий личному ключу Pr_k, используют для проверки подписи (например, верификации того, что подписанное эталонное хеш-значение было подписано правильным личным ключом, или даже для извлечения H_{ref} путем дешифрования $S(H_{ref})$ с помощью открытого ключа дешифрования, например, с помощью алгоритма RSA «Ривест-Шамир-Адлеман»).

Второй вариант способа нанесения маркировки, проиллюстрированный вариантом осуществления, показанным на фиг. 4, хорошо подходит для предоставления графических символов на множестве частей носителя, как, например,

- печать (как в случае альтернативы (ii) способа нанесения маркировки) текстового документа, содержащего множество страниц (например, N страниц отчета или контракта и т. д.), или

- отображение (как в случае альтернативы (i) способа нанесения маркировки) цифровой версии текстового документа, состоящего из N страниц, на экране в заданном формате (например, в формате Microsoft Word или pdf), страница за страницей,

при этом каждая из N ($N \geq 2$) страниц, маркированных на подложке, или каждая из N отображаемых страниц показывает определенный фрагмент удобочитаемых для человека графических символов HrGS(j) ($j \in \{1,\ldots,N\}$) и машиночитаемого представления соответствующих данных с исправлением ошибок MrECD(j): оба являются представлениями, полученными из фрагмента верифицируемых графических данных VGD(j) соответствующего определенного субблока верифицируемых графических данных VGDSB(j). В этих случаях согласно указанному второму варианту способа нанесения маркировки способ начинается 400 и (полный) блок графических данных GDB разделяют 410 блоком обработки на N субблоков GDSB(1),…, GDSB(N) (т. е. один субблок для каждой части носителя), при этом каждый субблок графических данных GDSB(j) форматируют для предоставления 415 соответствующего удобочитаемого для человека представления HrGS(j) его графических символов GS(j) в соответствующем субблоке удобочитаемых для человека графических данных HrGDSB(j). Для каждого субблока графических данных GDSB(j) (j=1,…,N) блок обработки генерирует соответствующие данные с исправлением ошибок субблока путем исправления 420 субблока графических данных GDSB (j) с помощью запрограммированного кода с исправлением ошибок ECC, а затем

образует 430 с помощью исправленных данных субблок данных с исправлением ошибок ECDSB(j). Блок обработки генерирует 440 машиночитаемое представление каждого субблока данных с исправлением ошибок ECDSB(j) как соответствующего субблока машиночитаемых данных с исправлением ошибок MrECDSB(j).Блок обработки затем форматирует каждый из субблоков HrGDSB(j) и MrECDSB(j), так что представление последнего на носителе отличается от удобочитаемого для человека представления HrGS(j) графических символов GS(j) первого, для предоставления 450 соответствующего субблока верифицируемых графических данных, символически написанного как VGDSB(j) = HrGDSB(j) + MrECDSB(j). В зависимости от выбранной альтернативы (i) или (ii) способа нанесения маркировки, данные субблоков VGDSB(j), j=1,…,N, отображают 460 на дисплее или наносят в виде маркировки 470 на подложку (например, печатают на листе бумаги, как на фиг. 1) согласно формату как верифицируемые графические данные VGD(j) (символически: VGD(j) = HrGS(j) + MrECD(j)), причем каждую маркировку M(j) VGD(j) предоставляют на части j подложки (например, печатают на j-ой странице документа, состоящего из N страниц), что говорит о завершении 480-490 процесса генерирования верифицируемых графических данных на носителе.

Несколько подвариантов вышеупомянутого второго варианта способа нанесения маркировки повышают уровень доверия в аутентичности удобочитаемых для человека графических символов или машиночитаемого представления данных с исправлением ошибок, предоставленных на носителе. Эти подварианты фактически являются первым и вторым подвариантами. Эти подварианты также используют квази-необратимость односторонних функций (например, хеш-функций, таких как хеш-функции SHA-256). В этих двух подвариантах, после осуществления этапов вышеупомянутого второго варианта способа нанесения маркировки, хеш-функцию H, запрограммированную в блоке обработки, дополнительно используют для получения хеш-значения цифрового представления графических символов или данных с исправлением ошибок (или некоторых частей этих данных). В связи с тем, что в указанном втором варианте способа нанесения маркировки блок графических данных GDB и

соответствующий блок данных с исправлением ошибок ECDB разделяют на N субблоков (соответствующих N частям носителя), существует несколько возможностей для определения для каждого субблока j (j=1,…,N) соответствующего хеш-значения субблока H(j), как объясняется выше: следует выбрать одну из этих возможностей, которая будет служить для вычисления N хеш-значений субблока в любом из этих подвариантов (а также в вариантах способа верификации).

В первом подварианте второго варианта способа нанесения маркировки блок обработки вычисляет для каждого субблока графических данных GDSB(j) (j=1,…,N) хеш-значение субблока H(j): например, в предпочтительном варианте осуществления полную конкатенацию субблока графических данных GDSB(j) и субблока данных с исправлением ошибок ECDSB(j) выбирают для хеш-значения субблока, т. е. H(j) = H(GDSB(j) ⊕ ECDSB(j)). В целом, хеш-значения субблока H(j), j=1,…,N, определяют согласно одной из следующих возможностей: можно иметь H(j) = H(GDSB(j)), или H(j) = H(ECDSB(j)), или взяв хеш-значение любой части конкатенации (GDSB(j) ⊕ ECDSB(j)) субблока графических данных GDSB(j) и субблока данных с исправлением ошибок ECDSB (j), т. е. где H(j) = H(часть (GDSB(j) ⊕ ECDSB(j)) (с ограничением относительно длины в битах уже упомянутой части).

Затем, машиночитаемое представление MrH(j) каждого хеш-значения субблока H(j) вычисляют блоком обработки и связывают с соответствующим субблоком верифицируемых графических данных VGDSB(j) (j=1,…,N). В результате, в дополнение к удобочитаемому для человека представлению j-ых графических символов субблока HrGS(j) и машиночитаемому представлению j-ых данных с исправлением ошибок субблока MrECD(j) (из субблока верифицируемых графических данных VGDSB(j)), j-ая страница документа дополнительно содержит машиночитаемое представление MrH(j) j-ого хеш-значения субблока. Этот подвариант позволяет дополнительно защитить графические данные субблока и соответствующие данные с исправлением ошибок субблока с помощью односторонней хеш-функции, поскольку любое изменение указанных

j-ых данных субблока не позволит извлекать содержимое данных MrH(j). Более того, это дополнительное преимущество достигается с помощью только ограниченных дополнительных данных, предоставленных на носителе в виде простого машиночитаемого представления хеш-значения субблока. В указанном первом подварианте второго варианта способа нанесения маркировки N хеш-значений субблока H(j) (j=1,…,N) затем используют для вычисления эталонного агрегированного хеш-значения H_{ref}. Как упомянуто выше, N хеш-значений субблока H(j), j = 1,…,N, можно вычислить на основании простых субблоков графических данных, т. е. H(j) ≡ H(GDSB(j)). Предпочтительно, хеш-значения субблока вычисляют на основании полной конкатенации субблоков: H(j) ≡ H(GDSB(j) ⊕ ECDSB(j)). Таким образом, любое изменение, даже одного бита, в аргументе любой из хеш-функций субблока H(j) (т. е. любое изменение в графических или машиночитаемых данных субблоков на носителе) будет генерировать разное значение агрегированного хеш-значения H_{ref}. В этом первом подварианте блок обработки конкатенирует все N хеш-значений субблока H(j), j=1,…,N, для получения эталонного агрегированного хеш-значения H_{ref} = H(1) ⊕ H(2) ⊕ … ⊕ H(N-1) ⊕ H(N) (символ ⊕ указывает на операцию конкатенации). Это эталонное хеш-значение H_{ref} дополнительно сохраняют в реестре (т. е. в сервере или базе данных, предпочтительно в блокчейне).

Необязательно, память блока обработки может дополнительно сохранять ключ для шифрования цифровых данных, предпочтительно личный ключ Pr_k в паре с открытым ключом Pu_k (т. е. для шифрования с асимметричным ключом), блок обработки, после конкатенации всех N хеш-значений субблока для получения эталонного агрегированного хеш-значения H_{ref} = H(1) ⊕ H(2) ⊕ … ⊕ H(N-1) ⊕ H(N), может дополнительно подписывать (т. е. шифровать) эталонное агрегированное хеш-значение H_{ref} с помощью ключа шифрования (предпочтительно личного ключа Pr_k) для получения подписи эталонного агрегированного хеш-значения $S(H_{ref})$. Затем эту подпись можно сохранять (например, в памяти блока обработки, или в базе данных, или в блокчейне) или дополнительно предоставлять на носителе. Эта последняя альтернатива

позволяет выполнять автономный процесс верификации, при условии что соответствующий ключ, предпочтительно открытый ключ Pu_k, связанный с личным ключом Pr_k, используют для проверки подлинности подписи (т. е. что она была получена с помощью правильного личного ключа Pr_k).

Во втором подварианте второго варианта способа нанесения маркировки, после вычисления N хеш-значений субблока H(j), j=1,…,N (так же, как в вышеупомянутом первом подварианте), эталонное агрегированное хеш-значение H_{ref} вычисляют блоком обработки как значение корневого узла R дерева, предпочтительно двоичного дерева. Это дерево имеет N хеш-значений субблока H(1), H(2),…, H(N-1), H(N) как листовых узлов, как проиллюстрировано на фиг. 5 (с примером простого двоичного дерева с N = 8). В данном случае также хеш-значения представляют значения, обычно получаемые с помощью односторонней функции (например, хеш-функции H() семейства SHA-256). Таким образом, дерево, как правило, основано на множестве вычисленных хеш-значений субблока H(j), j=1,…,N, и содержит узлы, расположенные согласно заданной упорядоченности узлов в дереве. Дерево содержит уровни узлов, начиная от листовых узлов a(1,j), j=1,…,N, соответственно, соответствующих множеству хеш-значений субблока H(1), H(2),…, H(N-1), H(N), и узлов, отличных от листовых, до корневого узла R дерева, причем каждый узел, отличный от листового (т. е. узел, содержащийся между листовым узлом и корневым узлом), дерева, соответствует хеш-значению конкатенации соответственных хеш-значений его дочерних узлов согласно упорядоченности конкатенации дерева, корневой узел R соответствует эталонному агрегированному хеш-значению H_{ref}, т. е. хеш-значению конкатенации хеш-значений узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева. В примере на фиг. 5, где N = 8, таким образом, имеют восемь листовых узлов (первый уровень дерева) a(1,j) = H(j), j=1,…,8, и для четырех значений узлов второго уровня: a(2,1) = H(a(1,1) $\oplus$ a(1,2)); a(2,2) = H(a(1,3) $\oplus$ a(1,4)); a(2,3) = H(a(1,5) $\oplus$ a(1,6)); a(2,4) = H(a(1,7) $\oplus$ a(1,8)). Для двух значений узлов третьего (предпоследнего) уровня: a(3,1) =

H(a(2,1) ⊕ a(2,2)) и a(3,2) = H(a(2,3) ⊕ a(2,4)). Таким образом, значение корневого узла R: R = H(a(3,1) ⊕ a(3,2)) ≡ H_{ref}.

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

Затем блок обработки вычисляет для каждого хеш-значения субблока H(j) (т. е. для каждого листового узла дерева a(1,j)), j=1,…,N, связанный ключ пути верификации субблока VPK(j). Ключ пути верификации субблока VPK(j), относящийся к листовому узлу a(1,j) (и, таким образом, к хеш-значению субблока H(j)), представляет собой ряд хеш-значений выбранных узлов, отличных от листовых, дерева, которые необходимы для извлечения значения корневого узла R, начиная от листового узла a(1,j). Выбранные узлы, отличные от листовых, фактически соответствуют определенному пути в дереве между листовым узлом a(1,j) и корневым узлом R. Ключ пути верификации субблока, связанный с заданным листовым узлом дерева, фактически представляет собой последовательность соответственных значений узлов, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и заданный листовой узел, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне. В примере простого двоичного дерева с восемью листовыми узлами a(1,1),…, a(1,8), показанном на фиг. 5, восемь ключей пути верификации субблока VPK(1),…, VPK(8) определяют следующим образом (согласно вышеупомянутому определению):

1) для заданного листового узла a(1,1) = H(1), связанный ключ пути верификации субблока представляет собой VPK(1) = {a(1,2),a(2,2),a(3,2)}, из которого можно извлечь значение корневой цифровой подписи R посредством

следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из заданного листового узла a(1,1) = H(1) и листового узла a(1,2) = H(2) в VPK(1) (a(1,2) представляет собой «другой листовой узел, имеющий такой же родительский узел», т. е. узел a(2,1), «что и заданный листовой узел», т. е. узел a(1,1)), получают значение родительского узла a(2,1) посредством a(2,1) = H(a(1,1) ⊕ a(1,2)) (т. е. a(2,1) = H(H(1) ⊕ H(2))),

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

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

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

Таким образом, на основании VPK(1) = {a(1,2),a(2,2),a(3,2)}, связанного с a(1,1), значение корневого узла дерева можно получить следующим образом: R = H(H(H(a(1,1) ⊕ a(1,2)) ⊕ a(2,2)) ⊕ a(3,2)).

2) для заданного листового узла a(1,2) = H(2), связанный ключ пути верификации субблока представляет собой VPK(2) = {a(1,1),a(2,2),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов

(выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из заданного a(1,2) = H(2) и a(1,1) = H(1) в VPK(2) (a(1,1) представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел a(2,1), что и заданный листовой узел, т. е. узел a(1,2)), получают значение родительского узла a(2,1) посредством a(2,1) = H(a(1,1) ⊕ a(1,2)),

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

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

Таким образом, на основании VPK(2) = {a(1,1),a(2,2),a(3,2)}, связанного с a(1,2), значение корневого узла дерева можно получить следующим образом: R = H(H(H(a(1,1) ⊕ a(1,2)) ⊕ a(2,2)) ⊕ a(3,2)).

3) для заданного листового узла a(1,3) = H(3), ключ пути верификации субблока представляет собой VPK(3) = {a(1,4),a(2,1),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,3) = H(3) и a(1,4) = H(4) в VPK(3) (a(1,4) представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел a(2,2), что и

заданный листовой узел, т. е. узел a(1,3)), получают значение родительского узла a(2,2) посредством a(2,2) = H(a(1,3) ⊕ a(1,4)),

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

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

Таким образом, значение корневого узла дерева можно получить как: R = H(H(a(2,1) ⊕ H(a(1,3) ⊕ a(1,4))) ⊕ a(3,2)).

4) для заданного листового узла a(1,4) = H(4), ключ пути верификации субблока представляет собой VPK(4) = {a(1,3),a(2,1),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,4) = H(4) и a(1,3) = H(3) в VPK(4), получают значение родительского узла a(2,2) посредством a(2,2) = H(a(1,3) ⊕ a(1,4)),

ii) из полученного a(2,2) и значения следующего узла в VPK(4), т. е. a(2,1) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,1) посредством a(3,1) = H(a(2,1) ⊕ a(2,2)),

iii) из полученного a(3,1) и значения следующего узла в VPK(4), т. е. a(3,2) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(H(a(2,1) ⊕ H(a(1,3) ⊕ a(1,4))) ⊕ a(3,2)).

5) для заданного узла a(1,5) = H(5), ключ пути верификации субблока представляет собой VPK(5) = {a(1,6),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,5) = H(5) и a(1,6) = H(6) в VPK(5), получают значение родительского узла a(2,3) посредством a(2,3) = H(a(1,5) ⊕ a(1,6)),

ii) из полученного a(2,3) и значения следующего узла в VPK(5), т. е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(5), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(H(a(1,5) ⊕ a(1,6)) ⊕ a(2,4))).

6) для заданного узла a(1,6) = H(6), ключ пути верификации субблока представляет собой VPK(6) = {a(1,5),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,6) = H(6) и a(1,5) = H(5) в VPK(6), получают значение родительского узла a(2,3) посредством a(2,3) = H(a(1,5) ⊕ a(1,6)),

ii) из полученного a(2,3) и значения следующего узла в VPK(6), т. е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(6), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(H(a(1,5) ⊕ a(1,6)) ⊕ a(2,4))).

7) для заданного узла a(1,7) = H(7), ключ пути верификации субблока представляет собой VPK(7) = {a(1,8),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,7) = H(7) и a(1,8) = H(8) в VPK(7), получают значение родительского узла a(2,4) посредством a(2,4) = H(a(1,7) ⊕ a(1,8)),

ii) из полученного a(2,4) и значения следующего узла в VPK(7), т. е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(7), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(a(2,3) ⊕ H(a(1,7) ⊕ a(1,8)))).

8) для заданного узла a(1,8) = H(8), ключ пути верификации субблока представляет собой VPK(8) = {a(1,7),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,8) = H(8) и a(1,7) = H(7) в VPK(8), получают значение родительского узла a(2,4) посредством a(2,4) = H(a(1,7) ⊕ a(1,8)),

ii) из полученного a(2,4) и значения следующего узла в VPK(8), т. е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(8), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(a(2,3) ⊕ H(a(1,7) ⊕ a(1,8)))).

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

- извлечения из последовательности значений узлов в ключе пути верификации субблока значения каждого другого листового узла дерева, имеющего такой же родительский узел, что и у заданного листового узла, и вычисления хеш-значения конкатенации заданного значения узла и, соответственно, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, извлеченного значения указанного каждого другого листового узла, тем самым получая хеш-значение указанного такого же родительского узла заданного листового узла;

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

.извлечения из последовательности значений узлов в ключе пути верификации субблока значения каждого другого узла, отличного от листового, дерева,

имеющего такой же родительский узел, что и у предыдущего такого же родительского узла, рассмотренного на предшествующем этапе, и

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

- вычисления хеш-значения конкатенации полученных значений узлов, отличных от листовых, соответствующих предпоследнему уровню узлов дерева согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая значение корневого узла дерева.

На следующем этапе второго подварианта второго варианта способа нанесения маркировки блок обработки генерирует машиночитаемое представление MrVPK(j) каждого ключа пути верификации субблока VPK(j) (j=1,…,N) и включает его одновременно с соответственно соответствующим субблоком удобочитаемых для человека графических данных HrGDSB(j) и субблоком машиночитаемых данных с исправлением ошибок MrECDSB(j) в субблок верифицируемых графических данных VGDSB(j). Субблок верифицируемых графических данных VGDSB(j) затем дополнительно форматируют для предоставления машиночитаемого представления указанного ключа пути верификации субблока, которое является отдельным от удобочитаемого для человека представления связанного субблока графических данных GDSB(j) и машиночитаемого представления связанного субблока данных с исправлением ошибок ECDSB(j), а затем предоставляют на носителе (как компонент соответствующих верифицируемых графических данных субблока). Таким образом, субблок верифицируемых графических данных теперь символически записывается: VGDSB(j) = HrGDSB(j) + MrECDSB(j) + MrVPK(j), j = 1,…,N. Наконец, далее осуществляют один из следующих этапов:

(iii) эталонное агрегированное хеш-значение H_{ref} = R сохраняют в реестре (предпочтительно в блокчейне),

или

(iv) эталонное агрегированное хеш-значение H_{ref} = R предоставляют в распоряжение пользователю.

Необязательно, H_{ref} можно подписывать с помощью личного ключа подписи Pr_k (сохраненного в памяти блока обработки) блоком обработки для получения подписи эталонного агрегированного хеш-значения $S(H_{ref})$, и подпись эталонного агрегированного хеш-значения $S(H_{ref})$ сохраняют (например, в реестре) или дополнительно предоставляют на носителе или в распоряжение пользователю. Затем, путем использования соответствующего открытого ключа Pu_k возможно проверить, является ли $S(H_{ref})$ подлинной.

В результате для каждого субблока графических данных GDSB(j) (j=1,…,N) блока графических данных GDB на носителе предоставлены соответствующие удобочитаемые для человека графические символы субблока вместе с соответствующими машиночитаемыми данными с исправлением ошибок субблока, которые аутентифицируются пользователем путем извлечения корневого значения R с помощью хеш-значения субблока H(j) и его соответствующего ключа пути верификации VPK(j), которые можно получить из данных, считываемых на носителе, соответственно, из удобочитаемых для человека графических символов субблока HrGS(j) и машиночитаемого представления ключа пути верификации субблока MrVPK(j).

Как ясно из вышеупомянутого примера, значение корневого узла R можно наконец извлечь из любого заданного значения листового узла путем вычисления хеш-значения конкатенации этого заданного значения листового узла только со значениями узлов, определенными в соответствующем ключе пути верификации субблока. Таким образом, объем данных в информации о верификации на основании ключа пути верификации (считываемого на

носителе), который необходим для извлечения значения корневого узла R, явно намного меньше, чем объем данных, необходимый для вычисления эталонного значения корневого узла H_{ref} на основании только всех значений листовых узлов (т. е. путем вычисления всех значений узлов, отличных от листовых, промежуточных уровней дерева): это является преимуществом настоящего изобретения с учетом ограничения ограниченного размера, доступного на машиночитаемом представлении данных (таком как, например, двухмерный штрих-код).

Таким образом, согласно настоящему изобретению переплетение хеш-значений всех оригинальных хеш-значений субблока, благодаря структуре дерева и использованию надежных односторонних функций для вычисления значений узлов дерева (таких как хеш-функции SHA-256 в вышеупомянутом варианте осуществления), вместе со значением корневого узла R дерева (которое может стать неизменным при сохранении в блокчейне), и включение машиночитаемых данных с исправлением ошибок и связанного машиночитаемого ключа пути верификации на носитель вместе с соответствующим удобочитаемым для человека представлением графических данных позволяют предотвращать фальсификацию данных на маркированном носителе с очень высоким уровнем надежности.

Вышеупомянутые варианты осуществления способа нанесения маркировки предоставляют на носителе (листе 100 бумаги или дисплее) удобочитаемые для человека графические символы вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые могут легко верифицироваться пользователем. Действительно, согласно способу верификации настоящего изобретения, иллюстративная блок-схема которого показана на фиг. 6, пользователь с помощью сканера, оснащенного блоком формирования изображения, блоком обработки сканера с памятью сканера, и дисплеем сканера, может проверить, были ли изменены удобочитаемые для человека графические символы HrGS на носителе или нет относительно оригинальных данных, или может даже извлечь оригинальные графические символы. В следующем

иллюстративном варианте осуществления способа верификации удобочитаемые для человека графические символы HrGS составляют текст, предоставленный на носитель согласно способу нанесения маркировки. Например, текст может быть напечатан на подложке (например, листе бумаги, как на фиг. 1) или отображен в электронном виде на экране. Блок формирования изображения сканера выполнен с возможностью отображения текста и соответствующего машиночитаемого представления данных с исправлением ошибок MrECD на носителе. Блок обработки сканера запрограммирован на осуществление обработки изображения носителя, взятого блоком формирования изображения, для извлечения текстовых данных и получения цифрового представления извлеченных текстовых данных как соответствующего блока сканированных графических данных SGDB. Блок обработки сканера также запрограммирован на осуществление обработки изображения машиночитаемого представления данных с исправлением ошибок MrECD на носителе, взятого блоком формирования изображения, для извлечения соответствующих сканированных данных с исправлением ошибок SECD, путем дополнительного использования запрограммированного (в блоке обработки сканера) машиночитаемого декодера, и получения цифрового представления сканированных данных с исправлением ошибок SECD как соответствующего блока сканированных данных с исправлением ошибок SECDB. Блок обработки сканера дополнительно запрограммирован на осуществление операций исправления ошибок блоков данных путем использования кода с исправлением ошибок ECC. Сканер может быть, например, простым смартфоном с камерой (как блоком формирования изображения) и приложениями для обработки изображения, декодирования и исправления ошибок, выполненными с возможностью запуска на его блоке обработки.

Общий процесс верификации, показанный на фиг. 6, с примером маркированного носителя на фиг. 1, начинается 600 путем:

- сканирования (через блок формирования изображения сканера) сканером текста HrGS 610 на носителе, т. е. текста 110 на текстовой области 120 листа 100

бумаги, и получения соответствующего блока сканированных графических данных SGDB 620 (т. е. цифрового представления сканированного текста); или

- сканирования машиночитаемого представления данных с исправлением ошибок MrECD 615 на носителе сканером, т. е. штрих-кода PDF417 130 на листе 100 бумаги, декодирования машиночитаемого представления данных с исправлением ошибок MrECD (с помощью запрограммированного машиночитаемого декодера) для извлечения соответствующих сканированных данных с исправлением ошибок SECD, и образования соответствующего блока сканированных данных с исправлением ошибок SECDB 625 (т. е. цифрового представления извлеченных SECD); и

- исправления 630 блока сканированных графических данных SGDB с помощью кода с исправлением ошибок ECC, запрограммированного в блоке обработки сканера (с использованием извлеченных SECD SECDB), и получения блока исправленных сканированных графических данных CSGDB 640, причем блок исправленных сканированных графических данных CSGDB содержит цифровое представление соответствующих исправленных удобочитаемых для человека графических символов CHrGS; и

- на этапе 650, осуществления по меньшей мере одной из трех альтернатив:

- (a) отображения 660 на дисплее сканера блока исправленных сканированных графических данных CSGDB как соответствующих исправленных удобочитаемых для человека графических символов CHrGS; или

- (b) указания 670 сканером (например, на дисплее сканера, или с помощью любого визуального или звукового сигнала, подаваемого сканером) того, содержит ли блок сканированных графических данных SGDB ошибку (на основании результата исправления 630); или

- (c) сохранения 680 данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных SGDB ошибку (на основании результата исправления 630), в памяти сканера.

Подача результата выбранного(-ых) альтернативы(альтернатив) (a), (b) и (c) приводит к завершению 690 процесса верификации.

Альтернатива (a) позволяет пользователю визуально сравнивать версию текста CHrGS, отображаемую на дисплее сканера, которая была исправлена с помощью запрограммированного кода с исправлением ошибок ECC, с использованием сканированных данных с исправлением ошибок SECD (полученных из машиночитаемого представления данных с исправлением ошибок MrECD), и (неисправленный) текст HrGS, сканированный на носителе. Предпочтительно, различие(-я) отображаемого текста со сканированным текстом можно выделять, чтобы помочь пользователю легко обнаружить и найти любое изменение в тексте (например, из-за изменения или мошенничества).

С помощью альтернативы (b) пользователь может быть предупрежден в случае любого различия между исправленным текстом CHrGS и текстом HrGS, сканированным на носителе.

Альтернатива (c) позволяет отслеживать любые существующие различия между исправленным текстом и текстом, сканированным на носителе. В качестве альтернативы, если сканер дополнительно оснащен средствами связи (например, смартфоном) и может быть подключен к внешнему серверу, данные результата сканирования можно сохранить в памяти сервера через канал связи.

Преимущество вышеупомянутого способа верификации заключается в том, что он позволяет автономно (т. е. без подключения к внешнему устройству через канал связи) проверить соответствие между текстом, предоставленным на носителе, как удобочитаемыми для человека графическими символами, и удобочитаемой для человека версией, которую можно получить из машиночитаемого представления данных с исправлением ошибок, считываемого на носителе: поскольку указанная версия является результатом исправления с помощью кода с исправлением ошибок (аналогично тому, как он уже использовался со способом нанесения маркировки для определения данных с исправлением ошибок, соответствующих тексту, предоставленному на носителе)

текста, считываемого сканером на носителе путем использования данных с исправлением ошибок, извлеченных из машиночитаемого представления, считываемого на носителе, и декодированных, посредством сканера. Однако, в случае если сканер дополнительно оснащен средствами связи (например, смартфоном) и может быть подключен к внешнему серверу, некоторые или все вышеупомянутые операции способа верификации декодирования и выполнения исправления ошибок блока данных можно осуществлять на (предназначенном) внешнем сервере.

Несколько вариантов способа верификации (соответственно коррелированных с первым и вторым вариантами способа нанесения маркировки, используемого для получения верифицируемых графических данных на носителе) позволяют пользователю выходить за пределы простой верификации текста (или, в более общем смысле, графических символов), предоставленного на носителе, путем дополнительной проверки аутентичности текста (и/или машиночитаемых данных).

В первом варианте способа верификации удобочитаемых для человека графических символов HrGS и машиночитаемого представления данных с исправлением ошибок, предоставленных на носителе согласно первому варианту способа нанесения маркировки, после осуществления этапов указанного способа верификации (см. фиг. 6), хеш-функция H дополнительно запрограммирована в блоке обработки сканера для вычисления хеш-значения блока данных (так же, как соответственно указано в первом варианте способа нанесения маркировки), сканер дополнительно подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, при этом эталонное хеш-значение H_{ref} сохраняют (как указано в первом варианте способа нанесения маркировки), и блок обработки сканера дополнительно вычисляет с помощью запрограммированной хеш-функции H хеш-значение сканирования H_{scan} как хеш-значение H(CSGDB) блока исправленных сканированных графических данных CSGDB, или хеш-значение H(SECDB) блока сканированных данных с исправлением ошибок SECDB, или хеш-значение

H(части CDB) любой части блока данных CDB ≡ (CSGDB ⊕ SECDB), полученной в результате конкатенации (CSGDB ⊕ SECDB) блока исправленных сканированных графических данных CSGDB и блока сканированных данных с исправлением ошибок SECDB (как объясняется выше).

Сканер дополнительно осуществляет следующие операции:

- сканер получает через свой блок связи (путем отправки запроса в реестр по каналу связи и приема ответа) эталонное хеш-значение H_{ref}, сохраненное в реестре, и

- затем блок обработки сканера проверяет, совпадает ли полученное эталонное хеш-значение H_{ref} с хеш-значением сканирования H_{scan}; и осуществляет по меньшей мере одну из операций:

(e) он указывает на результат операции проверки (например, через дисплей сканера), или

(f) он сохраняет результат операции проверки в памяти сканера.

Любое изменение относительно оригинального (подлинного) текста (как удобочитаемых для человека графических символов) удобочитаемого для человека текста, предоставленного на носителе, или содержимого его машиночитаемых данных с исправлением ошибок, предоставленных на носителе, будет генерировать несоответствие между эталонным хеш-значением H_{ref} и хеш-значением сканирования H_{scan}. Таким образом, этот вариант повышает уровень доверия к соответствию текста на носителе его оригинальной версии.

Второй вариант способа верификации, проиллюстрированный вариантом осуществления, показанным на фиг. 7, хорошо подходит в случае разделения полного набора графических символов на множество N подмножеств (где $N \geq 2$), причем каждое подмножество графических символов маркировано на соответствующей части подложки, как, например, текст, напечатанный (согласно альтернативе (ii) второго варианта способа нанесения маркировки) на

множестве страниц (например, N страниц отчета или контракта и т. д.), или отображаемый (согласно альтернативе (i) второго варианта способа нанесения маркировки) на экране в заданном формате (например, текстовый документ, состоящий из N страниц, в формате Microsoft Word или pdf), страница за страницей, при этом каждая маркированная часть подложки или каждая отображаемая страница демонстрирует определенное подмножество удобочитаемых для человека графических символов и машиночитаемого представления соответствующих данных с исправлением ошибок (оба являются представлениями, полученными из соответствующего определенного субблока верифицируемых графических данных).

В следующем иллюстративном варианте осуществления второго варианта способа верификации (см. фиг. 7) удобочитаемые для человека графические символы HrGS составляют текст, который предоставлен на носителе согласно второму варианту способа нанесения маркировки. Например, текст может быть напечатан на подложке (например, листе бумаги, как на фиг. 1) или отображен в электронном виде на экране. Блок формирования изображения сканера выполнен с возможностью формирования изображения каждой страницы из N страниц текста на носителе, т. е. каждых из (верифицируемых) удобочитаемых для человека графических символов HrGS(j) и машиночитаемого представления соответствующих данных с исправлением ошибок MrECD(j), предоставленных на j-ой странице (j = 1,…,N). Блок обработки сканера запрограммирован на осуществление обработки изображения j-ой страницы (j = 1,…,N) на носителе, взятого блоком формирования изображения, для извлечения сканированных текстовых данных из сформированного изображения удобочитаемых для человека графических символов HrGS(j) (т. е. сформированного изображения графических символов j-ого субблока) и получения цифрового представления извлеченных данных как соответствующего субблока сканированных графических данных SGDSB(j). Блок обработки сканера также запрограммирован на осуществление обработки изображения страницы j на носителе, взятого блоком формирования изображения, извлечение сканированных данных с исправлением ошибок SECD(j) из сформированного

изображения машиночитаемого представления данных с исправлением ошибок MrECD(j), путем использования машиночитаемого декодера, запрограммированного в блоке обработки сканера, и получения цифрового представления сканированных данных с исправлением ошибок SECD(j) как соответствующего субблока сканированных данных с исправлением ошибок SECDSB(j). Блок обработки сканера дополнительно запрограммирован на осуществление операций исправления ошибок блоков данных путем использования кода с исправлением ошибок ECC. Сканер может быть простым смартфоном с камерой (как блоком формирования изображения) и приложениями для обработки изображения, декодирования и исправления ошибок, выполненными с возможностью запуска на его блоке обработки.

Согласно вышеупомянутому варианту осуществления (фиг. 7) указанного второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок были предоставлены на носителе согласно второму варианту способа нанесения маркировки (как показано на фиг. 4), вышеупомянутый сканер начинает 700 выполнение для каждой страницы j (j= 1,…,N) документа следующих операций:

- сканирования 710 блоком формирования изображения сканера удобочитаемых для человека графических символов HrGS(j), предоставленных на странице j носителя, т. е. текста 110 на текстовой области 120 листа 100 бумаги, и получения 720 соответствующего субблока сканированных графических данных SGDSB(j) (т. е. цифрового представления сканированных удобочитаемых для человека графических символов); и

- сканирования 715 блоком формирования изображения сканера машиночитаемого представления данных с исправлением ошибок MrECD(j), предоставленных на странице j носителя, т. е. штрих-кода PDF417 130 на листе 100 бумаги, декодирования блоком обработки сканера сформированного изображения MrECD(j), с использованием запрограммированного машиночитаемого декодера, извлечения соответствующих сканированных

данных с исправлением ошибок SECD(j) и образования соответствующего субблока сканированных данных с исправлением ошибок SECDSB(j) 725 как цифрового представления сканированных данных с исправлением ошибок SECD(j);

- исправления 730 блоком обработки сканера субблока сканированных графических данных SGDSB (j) путем использования кода с исправлением ошибок ECC, запрограммированного в блоке обработки сканера (и использования извлеченных SECD(j) SECDSB(j)), и получения 740 субблока исправленных сканированных графических данных CSGDSB(j); и

- осуществления 750 по меньшей мере одной из трех альтернатив для каждой страницы j:

- (a) отображения 760 на дисплее сканера визуального представления (т. е. удобочитаемого для человека) субблока исправленных сканированных графических данных CSGDB(j) как соответствующих исправленных удобочитаемых для человека графических символов CGS(j); или

- (b) указания 770 сканером (например, на дисплее сканера, или с помощью любого визуального или звукового сигнала, подаваемого сканером) того, содержит ли субблок сканированных графических данных SGDB(j) ошибку (на основании результата исправления 730); или

- (c) сохранения 780 данных результата сканирования, указывающих на то, содержит ли субблок сканированных графических данных SGDB(j) ошибку (на основании результата исправления 730), в памяти сканера.

Подача результата выбранного(-ых) альтернативы(альтернатив) (a), (b) и (c) приводит к завершению 790 второго варианта процесса верификации каждой страницы документа. Если сканер дополнительно оснащен средствами связи (например, смартфоном) и может быть подключен к внешнему серверу, данные результата сканирования альтернативы (c) можно сохранить в памяти сервера через канал связи.

Настоящее изобретение также включает три подварианта вышеупомянутого второго варианта способа верификации. Во всех этих подвариантах, после осуществления этапов варианта осуществления второго варианта способа верификации, как показано на фиг. 7, односторонняя функция, в данном случае хеш-функция H, дополнительно запрограммирована в блоке обработки сканера для вычисления хеш-значения блока данных (так же, как соответственно указано в вариантах способа нанесения маркировки), и блок обработки сканера дополнительно вычисляет с помощью запрограммированной хеш-функции H N хеш-значений субблока сканирования $H_{scan}(j)$ (j=1,…,N), причем каждое хеш-значение субблока сканирования $H_{scan}(j)$ представляет собой хеш-значение как хеш-значение H(CSGDSB(j)) j-ого субблока исправленных сканированных графических данных CSGDSB(j), или хеш-значение H(SECDSB(j)) j-ого субблока сканированных данных с исправлением ошибок SECDSB(j), или хеш-значение H(часть CDB(j)) любой части блока данных CDB(j) ≡ (CSGDSB(j) ⊕ SECDSB(j)), полученной в результате конкатенации (CSGDSB(j) ⊕ SECDSB(j)) j-ого субблока исправленных сканированных графических данных CSGDB(j) и j-ого субблока сканированных данных с исправлением ошибок SECDSB(j). Использование вычисленных хеш-значений субблока сканирования $H_{scan}(j)$ является определенным в каждом из указанного первого, второго и третьего подвариантов второго варианта способа верификации, как подробно описано ниже.

В варианте осуществления первого подварианта варианта осуществления второго варианта способа верификации, в котором удобочитаемые для человека графические символы HrGS(j) и машиночитаемые данные с исправлением ошибок MrECD(j) на носителе были сгенерированы согласно первому подварианту второго варианта способа нанесения маркировки, хеш-функция и код с исправлением ошибок запрограммированы в блоке обработки сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления хеш-значения субблока H(j) на носителе блоком обработки сканера. Более того, сканер подключен к блоку связи сканера,

выполненному с возможностью установления связи через канал связи с реестром, в котором сохраняют эталонное агрегированное хеш-значение. Сканер вычисляет (см. выше) хеш-значения субблока сканирования $H_{scan}(j)$, $j=1,\ldots,N_{,,}$ в случае если это возможно (т. е. если все HrGS(j) и MrECD(j) являются считываемыми). В случае если невозможно вычислить хеш-значение субблока сканирования для некоторой страницы j, например, поскольку HrGS(j) и MrECD(j) на этой j-ой странице являются не считываемыми, сканер сканирует и декодирует машиночитаемое представление MrH(j) хеш-значения субблока H(j) на этой j-ой странице носителя и получает соответствующее декодированное хеш-значение субблока DH(j): это декодированное хеш-значение субблока затем будет служить как хеш-значение субблока сканирования, т. е. $H_{scan}(j) \equiv DH(j)$, для j-ой страницы. Это машиночитаемое представление j-ого хеш-значения субблока MrH(j) связывают с субблоком верифицируемых графических данных VGDSB(j), что соответствует удобочитаемым для человека графическим символам HrGS(j) и машиночитаемому представлению данных с исправлением ошибок MrECD(j), предоставленных на носителе. В результате, все хеш-значения субблока сканирования, необходимые для вычисления агрегированного хеш-значения для всех страниц носителя, являются доступными (либо как вычисленные хеш-значения сканирования $H_{scan}(j)$, либо как идентифицированные с декодированными хеш-значениями DH(j)).

Блок обработки сканера затем выполняет дополнительные операции:

- вычисления агрегированного хеш-значения сканирования H_{scan} путем конкатенации всех полученных хеш-значений сканирования (символ $\oplus$ представляет собой оператор конкатенации):

$$H_{scan} \equiv H_{scan}(1) \oplus H_{scan}(2) \oplus \ldots \oplus H_{scan}(N-1) \oplus H_{scan}(N).$$

- отправки блоком связи сканера через канал связи запроса на эталонное агрегированное хеш-значение в реестр и приема обратно эталонного агрегированного хеш-значения H_{ref};

- проверки того, совпадает ли принятое эталонное агрегированное хеш-значение H_{ref} с агрегированным значением сканирования H_{scan}, и указания результата операции проверки (например, посредством сообщения на дисплее сканера). В случае совпадения все страницы являются подлинными (т. е. соответствуют оригинальным страницам), даже если текст и машиночитаемые данные с исправлением ошибок на некоторых страницах не могли быть считаны (машиночитаемые представления хеш-значений субблока, однако, являются считываемыми). В случае несовпадения, по меньшей мере одна из страниц была изменена (например, по меньшей мере один из графических символов изменен или подделан): затем возможно извлечь такую страницу путем проверки того, совпадают ли хеш-значения субблока сканирования Hscan(j), полученные из данных субблока HrGS(j) и MrECD(j), с соответствующими декодированными хеш-значениями DH(j), j=1,…,N.

Этот подвариант позволяет независимо проверять сканером, является ли каждая страница документа, состоящая из N страниц, подлинной с помощью сканирования простого машиночитаемого представления хеш-значения субблока ограниченного размера.

В варианте осуществления второго подварианта второго варианта способа верификации удобочитаемые для человека графические символы HrGS(j), (j=1,…,N) и машиночитаемые данные с исправлением ошибок MrECD(j) на странице j (документа, состоящего из N страниц) на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, альтернатива (iii), сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, содержащим эталонное агрегированное хеш-значение H_{ref} (как значение корневого узла дерева, см. фиг. 5), хеш-функцию (такую же, что используется для вычисления N хеш-значений субблока H(j), и соответствующее эталонное агрегированное хеш-значение H_{ref}) запрограммировано в блоке обработки сканера. Сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления MrVPK(j)

(j=1,…,N) ключа пути верификации субблока VPK(j) на носителе и вычисления агрегированного хеш-значения сканирования H_{scan} из пары соответствующего хеш-значения субблока H(j) и ключа пути верификации субблока VPK(j), сканированного на носителе (в данном случае, рассматривают случай, где N = 8, с двоичным деревом, что соответствует примеру на фиг. 5 для документа, состоящего из 8 страниц). После вычисления с помощью хеш-функции (см. выше) хеш-значения субблока сканирования $H_{scan}(j)$, ($j\epsilon\{1,\ldots,N\}$) из сканированных верифицируемых графических данных на странице j документа, состоящего из N страниц, и согласно второму подварианту второго варианта способа нанесения маркировки (т. е. с таким же выбранным выбором H(CSGDSB(j)), или H(SECDSB(j) или H(части CDB(j) для вычисления хеш-значения субблока, используемого как листовые узлы дерева), сканер выполняет дополнительные операции:

- сканирования машиночитаемого представления MrVPK(j) ключа пути верификации субблока VPK(j) на j-ой странице носителя (что соответствует j-ому субблоку исправленных сканированных графических данных CSGDSB(j)) и извлечения соответствующего сканированного ключа пути верификации субблока SVPK(j) блоком обработки сканера;

- вычисления блоком обработки сканера агрегированного хеш-значения сканирования H_{scan} с помощью вычисленного хеш-значения субблока сканирования $H_{scan}(j)$ и сканированного ключа пути верификации субблока SVPK(j), полученного путем сканирования j-ой страницы документа, как объясняется ниже:

.Если j = 1 (первая страница документа), и как объясняется выше касательно варианта осуществления второго подварианта второго варианта способа нанесения маркировки (см. также иллюстративное двоичное дерево на фиг. 5), хеш-значение субблока $H_{scan}(1)$, полученное как указано выше (т. е. из первого субблока исправленных сканированных графических данных CSGDB(1) и/или первого субблока сканированных данных с исправлением ошибок SECDSB(1))

считается значением первого листового узла a(1,1) двоичного дерева (выбирается такая же упорядоченность узлов и упорядоченность конкатенации дерева, что и в вышеупомянутом варианте осуществления второго подварианта второго варианта способа нанесения маркировки), извлеченный сканированный ключ пути верификации субблока SVPK(1) содержит три значения узлов: SVPK(1)={a(1,2),a(2,2),a(3,2)}, таким образом, хеш-значение сканирования H_{scan}, которое можно получить из сканирования верифицируемых графических данных первой страницы, вычисляют следующим образом

$$H_{scan} = H(H(H(a(1,1) \oplus a(1,2)) \oplus a(2,2)) \oplus a(3,2))$$

$$= H(H(H(H_{scan}(1) \oplus a(1,2)) \oplus a(2,2)) \oplus a(3,2))$$

.Если j = 2, где SVPK(2) = {a(1,1), a(2,2), a(3,2)},

$$H_{scan} = H(H(H(a(1,1) \oplus H_{scan}(2)) \oplus a(2,2)) \oplus a(3,2))$$

.Если j = 3, где SVPK(3) = {a(1,4),a(2,1),a(3,2)},

$$H_{scan} = H(H(a(2,1) \oplus H(H_{scan}(3) \oplus a(1,4))) \oplus a(3,2))$$

.Если j = 4, где SVPK(4) = {a(1,3),a(2,1),a(3,2)}

$$H_{scan} = H(H(a(2,1) \oplus H(a(1,3) \oplus H_{scan}(4))) \oplus a(3,2))$$

.Если j = 5, где SVPK(5) = {a(1,6),a(2,4),a(3,1)}

$$H_{scan} = H(a(3,1) \oplus H(H(H_{scan}(5) \oplus a(1,6)) \oplus a(2,4)))$$

.Если j = 6, где SVPK(6) = {a(1,5),a(2,4),a(3,1)}

$$H_{scan} = H(a(3,1) \oplus H(H(a(1,5) \oplus H_{scan}(6)) \oplus a(2,4)))$$

.Если j = 7, где SVPK(7) = {a(1,8),a(2,3),a(3,1)},

$$H_{scan} = H(a(3,1) \oplus H(a(2,3) \oplus H(H_{scan}(7) \oplus a(1,8))))$$

.Если j = 8, где SVPK(8) = {a(1,7),a(2,3),a(3,1)},

$$H_{scan} = H(a(3,1) \oplus H(a(2,3) \oplus H(a(1,7) \oplus H_{scan}(8)))).$$

- далее, получения эталонного агрегированного хеш-значения H_{ref} (т. е. значения корневого узла R дерева), сохраненного в реестре, блоком связи сканера и каналом связи, и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение H_{ref} с агрегированным хеш-значением сканирования H_{scan}, для j=1,…,N; и

- указания результата операции проверки (например, на дисплее сканера).

Этот подвариант способа верификации позволяет обнаруживать любую ошибку на каждой странице документа только с небольшим объемом данных, поскольку любое изменение в содержимом страницы приводит в результате к несовпадению между эталонным агрегированным хеш-значением H_{ref} и хеш-значением сканирования H_{scan}, полученным из верифицируемых графических данных, сканированных на этой странице. Более того, этот способ является надежным, поскольку исправленную версию сканированных графических данных используют для вычисления хеш-значений субблока $H_{scan}(j)$ j-ой страницы, j=1,…,N.

В варианте осуществления третьего подварианта второго варианта способа верификации используют такое же двоичное дерево документа, состоящего из N = 8 страниц, а также такой же способ вычисления хеш-значений субблока сканирования $H_{scan}(j)$ (j=1,…,N) и хеш-значений сканирования H_{scan}, что и в вышеупомянутом примере второго подварианта второго варианта способа верификации. В этом варианте осуществления удобочитаемые для человека графические символы HrGS(j) и машиночитаемые данные с исправлением ошибок MrECD(j) на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, альтернатива (iv), эталонное агрегированное хеш-значение H_{ref} сохраняют в памяти сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования

машиночитаемого представления ключа пути верификации субблока VPK(j) на носителе и вычисления агрегированного хеш-значения $H_{scan}(j)$ из пары соответствующего хеш-значения субблока и ключа пути верификации субблока. Согласно этому варианту осуществления, после осуществления этапов указанного второго варианта способа верификации и вычисления хеш-значения субблока сканирования $H_{scan}(j)$ (j=1,…,N), как упомянуто выше, сканер выполняет дополнительные этапы:

- сканирования сканером машиночитаемого представления MrVPK(j) ключа пути верификации субблока VPK(j) на j-ой странице, предоставленной на носителе (что соответствует j-ому субблоку исправленных сканированных графических данных CSGDSB(j), например, полученному из сканированных верифицируемых графических данных, предоставленных на j-ой странице документа), и извлечения соответствующего сканированного ключа пути верификации субблока SVPK(j) блоком обработки сканера;

- вычисления агрегированного хеш-значения сканирования H_{scan} с помощью вычисленного хеш-значения субблока сканирования $H_{scan}(j)$ и сканированного ключа пути верификации субблока SVPK(j), полученного путем сканирования j-ой страницы документа (см. выше, подробное вычисление, относящееся ко второму подварианту варианта осуществления второго варианта способа верификации);

- получения эталонного агрегированного хеш-значения H_{ref}, сохраненного в памяти сканера;

- проверки блоком обработки сканера того, совпадает ли полученное эталонное агрегированное хеш-значение H_{ref} с агрегированным хеш-значением сканирования H_{scan} для j-ой страницы (j=1,…,N); и

- указания результата операции проверки (через дисплей сканера).

Этот подвариант способа верификации позволяет обнаруживать любую ошибку надежным автономным способом на каждой странице документа только с

небольшим объемом данных, поскольку любое изменение в содержимом страницы приводит в результате к несовпадению между эталонным агрегированным хеш-значением H_{ref} и хеш-значением сканирования H_{scan}, полученным из верифицируемых графических данных, сканированных на этой странице. Действительно, способ только использует данные (ограниченного размера), сохраненные в памяти сканера (т. е. H_{ref}), для проверки того, совпадает ли эталонное агрегированное хеш-значение H_{ref} с хеш-значением сканирования H_{scan}.

Вариант осуществления альтернативного варианта способа верификации иллюстрирует приложение настоящего изобретения для верификации удобочитаемых для человека графических символов и соответствующих машиночитаемых данных с исправлением ошибок, сгенерированных в компьютере, подключенном к дисплею, процессором, запрограммированным на осуществление этапов вышеупомянутого способа нанесения маркировки, альтернатива (i). Компьютер имеет приложение для сканирования, запрограммированное в его процессоре, которое выполнено с возможностью сканирования отображаемых удобочитаемых для человека графических символов и машиночитаемых данных с исправлением ошибок.

Таким образом, компьютер отображает сгенерированные удобочитаемые для человека графические символы HrGS и соответствующие машиночитаемые данные с исправлением ошибок MrECD, и приложение для сканирования, запущенное в процессоре компьютера, затем осуществляет следующие операции:

- сканирования отображаемых удобочитаемых для человека графических символов HrGS для получения блока сканированных графических данных SGDB, причем этот блок сканированных графических данных представляет собой цифровое представление сканированных удобочитаемых для человека графических символов;

- сканирования отображаемых машиночитаемых данных с исправлением ошибок MrECD и с помощью машиночитаемого декодера приложения для сканирования, запущенного в процессоре компьютера, декодирования сканированных машиночитаемых данных с исправлением ошибок MrECD для получения соответствующих сканированных данных с исправлением ошибок SECD в блоке сканированных данных с исправлением ошибок SECDB;

- исправления блока сканированных графических данных SGDB с помощью кода с исправлением ошибок ECC приложения для сканирования, запущенного в процессоре компьютера, с использованием сканированных данных с исправлением ошибок SECD блока сканированных данных с исправлением ошибок SECDB для получения соответствующего блока исправленных сканированных графических данных CSGDB; и

- осуществления по меньшей мере одного из следующих этапов:

(a) отображения визуального представления блока исправленных сканированных графических данных CSGDB как исправленных удобочитаемых для человека графических символов CHrGS на дисплее, или

(b) отображения сообщения, указывающего на то, содержит ли блок сканированных графических данных SGDB ошибку (на основании результата этапа исправления SGDB), или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных SGDB ошибку, в памяти компьютера.

На этапе (a) части первоначально отображаемых удобочитаемых для человека графических символов HrGS (перед запуском приложения для сканирования), которые были исправлены с помощью приложения для сканирования, предпочтительно выделяют для упрощения идентификации и местоположения ошибок в изначально отображаемых HrGS пользователем компьютера.

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

Описание, измененное по ст. 34 PCT

СЕРТИФИЦИРОВАННЫЙ ТЕКСТОВЫЙ ДОКУМЕНТ

Область техники, к которой относится изобретение

Настоящее изобретение относится к области техники способов и систем безопасности и защиты от мошенничества. В частности, настоящее изобретение относится к защите данных от подделки или фальсификации, например, таких как текстовые данные ценного документа (оцифрованного или напечатанного).

Предпосылки создания изобретения

Проблемы подделки и фальсификации цифровых файлов или напечатанных документов являются хорошо известными и серьезными, и их количество постоянно растет. Хорошо известным является пример фальсификации данных, маркированных на оригинальном (цифровом или материальном) документе, таком как документ, удостоверяющий личность, или диплом, и дело обстоит еще хуже, если рассматривать цифровую копию оригинального (возможно, подлинного) цифрового/материального документа. Простое отслеживание идентификаторов, таких как серийные номера, или даже включение некоторых цифровых водяных знаков, как правило, является слабым решением, поскольку фальсификаторы могут легко скопировать такие номера или цифровые водяные знаки.

Существует множество известных методов защиты содержимого цифрового или физического документа от подделки. Например, взяв хеш-значение цифровых данных из оригинального цифрового документа или из оцифрованной версии оригинального физического документа (например, путем сканирования документа и извлечения текстовых данных с помощью программного обеспечения сканера OCR) и сохранения хеш-значения в реестре (например, простая база данных или блокчейн). Затем путем сканирования содержимого

данных исследуемого документа, визуально представленного на физическом носителе (например, носитель может быть листом бумаги, на котором напечатаны данные), и вычисления хеш-значения указанного содержимого данных, а затем сравнения вычисленного хеш-значения с хеш-значением, сохраненным в реестре, соответствующем оригинальному документу, можно обнаружить изменение содержимого данных. Однако, недостатком этого способа является то, что из-за некоторого изменения визуального представления на носителе содержимого документа, даже если этот документ является подлинным, вычисленное хеш-значение может отличаться от сохраненного хеш-значения. Это различие также может быть связано со способом выполнения операции сканирования или даже зависеть от типа используемого сканера (два разных сканера могут дать два противоположных результата). Это также верно для цифрового документа, отображаемого на носителе, таком как экран (например, компьютера): даже если содержимое документа является подлинным, любое изменение отображаемого содержимого будет генерировать, при сканировании отображаемого содержимого для верификации, хеш-значение, отличное от сохраненного хеш-значения. Таким образом, на практике сканирование документа и вычисление хеш-значения захваченного изображения не работают, потому что каждый раз при сканировании документа обычно получается другое хеш-значение. Использование сканера OCR («Оптическое распознавание символов») перед вычислением хеш-значения не решает вышеупомянутую проблему, поскольку не существует системы OCR, которая работает на 100%: например, если просто точка становится запятой, или буква «l» (т. е. L) становится «1» (то есть единицей), вычисленное хеш-значение будет другим.

Некоторые существующие методы защиты бумажных документов (например, сертификатов, дипломов, контрактов и т. д.) с использованием лишь небольшого объема информации, извлеченной из документа, включают создание двухмерного штрих-кода (например, QR-кода), размещение извлеченной информации внутри двухмерного штрих-кода и его печать на документе. Каждый раз при считывании двухмерного штрих-кода получается один и тот же

результат, но с недостатком, заключающимся в том, что информацию, включенную в штрих-код, необходимо сравнивать с информацией, напечатанной на документе. Более того, если кто-то хочет защитить, например, полнотекстовую страницу, необходимо поместить полный текст в штрих-код, и, таким образом, штрих-код становится огромным по размеру и требует много места на странице, что воспринимается читателем как что-то нарушающее обычный порядок (так что на практике полный текст, который может быть закодирован, имеет ограниченный размер), и становится необходимым (и утомительным) сравнивать несколько тысяч символов между напечатанным текстом и текстом, декодированным с помощью штрих-кода.

В документах US 6047093 A, EP 2048867 и US 2004/145661, как известно, раскрыто определение ошибок в тексте, напечатанном на документе, и образование информации на нем.

Краткое описание изобретения

Настоящее изобретение направлено на устранение вышеупомянутых недостатков предшествующего уровня техники, касающихся подделки и фальсификации цифровых файлов или напечатанных документов, путем обеспечения автоматического обнаружения любого изменения в расположении маркированных (соответственно отображаемых) графических символов (например, текста) в отношении к оригинальному расположению, и, в частности, устранение избыточности между данными внутри кода и напечатанным (соответственно отображаемым) текстом, избегая бремени визуального сравнения текста внутри кода с напечатанным (или отображаемым) текстом, одновременно решая проблему слишком большого размера кода, когда размер данных для напечатанного (или отображаемого) текста велик.

Таким образом, настоящее изобретение направлено на обеспечение точного и надежного способа получения на материальном носителе, таком как дисплей (например, экран компьютера) или подложка (например, лист бумаги, этикетка, упаковка), видимых графических символов (например, текстовых символов или

глиф), соответствие которых аутентичным эталонным графическим символам пользователь может легко проверить, считывая указанные видимые графические символы, и это позволяет устранить недостатки предшествующего уровня техники. Графические символы являются удобочитаемыми для человека и взяты из заданного конечного набора графических символов (например, таких как текстовые символы из алфавита). Таким образом, пользователь может верифицировать удобочитаемые для человека графические символы, отображаемые или маркированные на подложке согласно настоящему изобретению, и любая попытка изменить любую часть графических символов может быть обнаружена.

Таким образом, настоящее изобретение относится к «способу нанесения маркировки», т. е. способу генерирования на носителе верифицируемых графических данных с использованием заданного конечного набора графических символов, причем носитель является дисплеем или подложкой, включающему этапы:

- сохранения в памяти блока обработки блока графических данных, содержащего цифровое представление графических символов;

- обработки блоком обработки цифрового представления графических символов сохраненного блока графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки, для генерирования данных с исправлением ошибок в соответствующем блоке данных с исправлением ошибок;

- форматирования блока графических данных и блока данных с исправлением ошибок блоком обработки для предоставления, соответственно, в блоке удобочитаемых для человека графических данных удобочитаемого для человека представления графических символов блока графических данных и в блоке машиночитаемых данных с исправлением ошибок машиночитаемого представления данных с исправлением ошибок блока данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических

символов блока графических данных для получения соответствующего блока верифицируемых графических данных, содержащего указанный блок удобочитаемых для человека графических данных и указанный блок машиночитаемых данных с исправлением ошибок; и

(i) отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок полученного блока верифицируемых графических данных на дисплее, подключенном к блоку обработки, или

(ii) нанесения маркировки на подложку устройством для нанесения маркировки, подключенным к блоку обработки и оснащенным блоком контроля, выполненным с возможностью контроля операции нанесения маркировки на основании данных, принятых от блока обработки, в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок блока верифицируемых графических данных, принятого от блока обработки,

с предоставлением тем самым на носителе удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые верифицируются пользователем.

Машиночитаемое представление данных с исправлением ошибок может быть любым из буквенно-цифрового представления или представления в виде штрих-кода (одномерный штрих-код, или двухмерный штрих-код, такой как, например, код DataMatrix или QR-код). Предпочтительно, штрих-код может быть обычным линейным штрих-кодом PDF417, который можно считывать простым линейным сканером, проводимым по штрих-коду. Предпочтительно, графические символы могут быть текстовыми символами, а конечный набор графических символов - алфавитом. Предпочтительно, устройство для нанесения маркировки может быть принтером (например, струйным принтером), а подложка может быть листом бумаги или этикеткой. Также предпочтительно, чтобы код с исправлением ошибок мог быть кодом с исправлением ошибок Рида-Соломона.

В первом варианте вышеупомянутый способ нанесения маркировки может включать дополнительные этапы:

- вычисления с помощью хеш-функции, запрограммированной в блоке обработки, хеш-значения блока графических данных, или блока данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока графических данных и блока данных с исправлением ошибок; и

- сохранения вычисленного хеш-значения как эталонного хеш-значения в реестре.

Хеш-функция является хорошо известным примером односторонней функции, т. е. функции, которую легко вычислить, но трудно инвертировать(см., например, S. Goldwasser and M. Bellare “Lecture Notes on Cryptography”, MIT, июль 2008 г., http://www-cse.ucsd.edu/users/mihir). Предпочтительно, криптографическая хеш-функция может принадлежать семейству SHA-2, как, SHA-256, например, задавая хеш-значения размером 256 битов: данная функция практически необратима и устойчива к коллизиям, то есть вероятность того, что две разные группы входных данных приведут к одним и тем же выходным данным, ничтожна. Также предпочтительно, чтобы реестр мог представлять собой блокчейн, который преимущественно обеспечивает неизменяемую запись данных. Необязательно, может быть дополнительный этап подписывания вычисленного эталонного хеш-значения с помощью личного ключа подписи блоком обработки для получения соответствующего подписанного эталонного хеш-значения и сохранения или дальнейшего предоставления на носителе подписанного эталонного хеш-значения. С помощью этой альтернативы пользователь, имеющий открытый ключ, соответствующий личному ключу, может проверить, что подписанное эталонное хеш-значение, считанное на носителе, является подлинным, поскольку оно подписано правильным личным ключом.

Во втором варианте вышеупомянутого способа нанесения маркировки носитель содержит множество частей, и блок верифицируемых графических данных разделяют на одинаковое множество субблоков верифицируемых графических данных, и соответствующие удобочитаемые для человека графические символы и машиночитаемое представление данных с исправлением ошибок, соответственно, распределяют вместе на соответствующие части носителя, посредством следующих этапов, на которых:

- блок графических данных разделяют на множество субблоков графических данных, и каждый субблок графических данных форматируют для предоставления удобочитаемого для человека представления его графических символов в соответствующем субблоке удобочитаемых для человека графических данных;

- для каждого субблока графических данных цифровое представление его графических символов извлекают и обрабатывают с помощью кода с исправлением ошибок для генерирования соответствующих данных с исправлением ошибок в субблоке данных с исправлением ошибок;

- каждый субблок данных с исправлением ошибок форматируют для предоставления в соответствующем субблоке машиночитаемых данных с исправлением ошибок машиночитаемого представления соответствующих данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов соответствующего субблока удобочитаемых для человека графических данных для получения соответствующего субблока верифицируемых графических данных, содержащего указанный субблок удобочитаемых для человека графических данных и указанный субблок машиночитаемых данных с исправлением ошибок; и

- на этапе (i), отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением

ошибок каждого полученного субблока верифицируемых графических данных на дисплее, или

- на этапе (ii), нанесения маркировки на подложку устройством для нанесения маркировки в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок каждого субблока верифицируемых графических данных, принятого блоком контроля от блока обработки,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые верифицируются пользователем.

Данный второй вариант способа нанесения маркировки для генерирования верифицируемых графических символов на носителе особенно адаптирован в случае документа, состоящего из нескольких страниц текста (т. е. носитель имеет множество частей): полный текст разделяют на множество частей, причем каждая часть текста соответствует странице текста и, таким образом, каждая страница документа, предусмотренная на носителе, содержит удобочитаемое для человека представление графических символов соответствующего субблока графических данных вместе с отдельным машиночитаемым представлением данных с исправлением ошибок соответствующего субблока данных с исправлением ошибок (например, в виде штрих-кода PDF417, показанного на фиг. 1).

С целью обеспечения возможности пользователю дополнительного определения того, являются ли удобочитаемые для человека графические символы и соответствующий субблок машиночитаемых данных с исправлением ошибок, считанный на носителе (т. е. на части носителя, соответствующей субблоку графических данных блока графических данных) аутентичными или нет, вышеупомянутый второй вариант осуществления способа нанесения маркировки

может дополнительно включать признаки одного из следующих двух подвариантов.

Согласно первому подварианту второго варианта способа нанесения маркировки,

- хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

- для каждого хеш-значения субблока вычисляют соответствующее машиночитаемое представление указанного хеш-значения субблока;

- одновременно с каждым субблоком верифицируемых графических данных, соответствующее машиночитаемое представление хеш-значения субблока дополнительно предоставляют на соответствующей части носителя;

- эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как конкатенацию всех вычисленных хеш-значений субблоков; и

- эталонное агрегированное хеш-значение сохраняют в реестре,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

Согласно второму подварианту второго варианта способа нанесения маркировки,

- хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических

данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

- эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как значение корневого узла дерева, имеющего вычисленные хеш-значения субблоков как значения листовых узлов, причем дерево содержит узлы, расположенные согласно заданной упорядоченности узлов в дереве, указанное дерево содержит уровни узлов, начиная от листовых узлов до корневого узла, причем каждое значение узла, отличного от листового, дерева соответствует хеш-значению конкатенации соответственных значений узлов его дочерних узлов согласно упорядоченности конкатенации дерева, значение корневого узла соответствует хеш-значению конкатенации значений узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

- для каждого хеш-значения субблока связанный ключ пути верификации субблока определяют как ряд хеш-значений выбранных узлов, отличных от листовых, дерева, необходимых для извлечения значения корневого узла из указанного хеш-значения субблока;

- машиночитаемое представление каждого ключа пути верификации субблока включают, одновременно с соответственно соответствующим субблоком графических данных и субблоком данных с исправлением ошибок, в субблок верифицируемых графических данных, причем субблок верифицируемых графических данных дополнительно форматируют для предоставления машиночитаемого представления указанного ключа пути верификации субблока отдельно от удобочитаемого для человека представления связанного субблока графических данных и машиночитаемого представления связанного субблока данных с исправлением ошибок; и

(iii) эталонное агрегированное хеш-значение сохраняют в реестре, или

(iv) эталонное агрегированное хеш-значение предоставляют в распоряжение пользователя,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

Настоящее изобретение также относится к «способу верификации», соответствующему вышеупомянутому «способу нанесения маркировки», т. е. способу верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемым представлением данных с исправлением ошибок на носителе, которые были сгенерированы согласно вышеупомянутому способу генерирования верифицируемых графических символов на указанном носителе, включающему этапы:

- сканирования сканером, оснащенным блоком формирования изображения, блоком обработки сканера, имеющим память сканера и подключенным к дисплею сканера, удобочитаемых для человека графических символов на носителе для получения путем обработки изображения сканированных удобочитаемых для человека графических символов блока сканированных графических данных, представляющего собой цифровое представление указанных сканированных удобочитаемых для человека графических символов;

- сканирования сканером машиночитаемого представления данных с исправлением ошибок на носителе для получения с помощью машиночитаемого декодера, запрограммированного в блоке обработки сканера, соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок, причем блок сканированных данных с исправлением ошибок представляет собой цифровое представление указанных сканированных данных с исправлением ошибок;

- исправления блока сканированных графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки сканера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как соответствующих исправленных удобочитаемых для человека графических символов на дисплее сканера, или

(b) указания сканером того, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти сканера.

Таким образом, согласно настоящему изобретению пользователь может непосредственно визуализировать на дисплее сканера (альтернатива (a)) оригинальные графические символы (например, оригинальный текст документа) благодаря исправлению сканированного текста, а затем легко сравнивать отображаемые графические символы (т. е. исправленные удобочитаемые для человека графические символы) с графическими символами на носителе и обнаруживать любые изменение или мошенничество.

Сканер может быть специально предназначенным устройством или может быть простым смартфоном, оснащенным камерой и имеющим запрограммированное приложение, выполненное с возможностью запуска в процессоре указанного смартфона и выполнения этапов вышеупомянутого способа верификации графических символов и соответствующих машиночитаемых данных с исправлением ошибок, предоставленных на носителе. Некоторые этапы способа верификации можно также выполнять на удаленном сервере, связанном со сканером: например, сканер может отправлять блок сканированных графических данных и машиночитаемые данные с исправлением ошибок на сервер,

подходящим образом запрограммированные средства обработки сервера могут затем выполнять этапы получения соответствующих сканированных данных с исправлением ошибок, исправления блока сканированных графических данных (с помощью кода с исправлением ошибок, запрограммированного в сервере) с использованием сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных и отправки блока исправленных сканированных графических данных в сканер (возможно с сообщением того, содержит ли блок сканированных графических данных ошибку, или сохранением данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, на сервере).

Первый вариант вышеупомянутого способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно первому варианту способа нанесения маркировки, причем хеш-функция запрограммирована в блоке обработки сканера, и сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включает дополнительные этапы:

- вычисления согласно первому варианту способа нанесения маркировки с помощью хеш-функции, запрограммированной в блоке обработки сканера, хеш-значения сканирования блока исправленных сканированных графических данных, или блока сканированных данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока исправленных сканированных графических данных и блока сканированных данных с исправлением ошибок;

- получения эталонного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное хеш-значение с хеш-значением сканирования; и

(e) указания результата операции проверки, или

(f) сохранения результата операции проверки в памяти сканера.

Таким образом, даже при изменении одного бита данных в данных, оригинально предоставленных на носителе, хеш-значение сканирования будет сильно отличаться от эталонного хеш-значения, и изменение будет обнаружено.

Во втором варианте вышеупомянутого способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно второму варианту способа нанесения маркировки,

- операция сканирования удобочитаемых для человека графических символов на носителе включает сканирование графических символов соответствующего субблока графических данных для получения путем обработки изображения соответствующего субблока сканированных графических данных как цифрового представления сканированных графических символов субблока;

- операция сканирования машиночитаемых данных с исправлением ошибок на носителе включает сканирование данных с исправлением ошибок соответствующего субблока данных с исправлением ошибок для получения соответствующего субблока сканированных данных с исправлением ошибок;

- операция исправления блока сканированных графических данных включает исправление графических данных субблока сканированных графических данных с использованием соответствующего субблока сканированных данных с исправлением ошибок для получения соответствующего субблока исправленных сканированных графических данных; и

- операция (a) отображения визуального представления блока исправленных сканированных данных включает отображение визуального представления субблока исправленных сканированных графических данных;

- операция (b) указания того, содержит ли блок сканированных графических данных ошибку, включает указание того, содержит ли субблок сканированных графических данных ошибку;

- операция (c) сохранения данных результата сканирования включает сохранение того, содержит ли субблок сканированных графических данных ошибку.

Первый подвариант второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно первому подварианту второго варианта способа нанесения маркировки, хеш-функция и код с исправлением ошибок запрограммированы в блоке обработки сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления хеш-значения субблока на носителе блоком обработки сканера, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включает дополнительные этапы:

- вычисления для каждой части носителя с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования соответствующего субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока исправленных сканированных графических данных и указанного субблока сканированных данных с исправлением ошибок;

- в случае если невозможно вычислить хеш-значение субблока сканирования для части носителя, сканирования и декодирования машиночитаемого представления хеш-значения субблока на указанной части носителя для получения соответствующего декодированного хеш-значения субблока, а также

использования этого декодированного хеш-значения субблока как хеш-значения субблока сканирования для этой части носителя;

- вычисления агрегированного хеш-значения сканирования как конкатенации всех хеш-значений субблока сканирования;

- получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

- указания результата операции проверки сканером.

Данный первый подвариант второго варианта способа нанесения маркировки позволяет проверять аутентичность графических символов всех считываемых частей носителя, даже если некоторая(-ые) часть(-и) является(являются) несчитываемой(-ыми) (например, благодаря сильному изменению графических символов и/или данных с исправлением ошибок, предоставленных на указанной(-ых) части(-ях)), путем извлечения исправленного агрегированного хеш-значения. Действительно, если хеш-значение субблока сканирования нельзя вычислить для определенной части носителя, его все еще можно получить путем считывания и декодирования машиночитаемого представления хеш-значения субблока на указанной части носителя, и использовать декодированное хеш-значение в конкатенации всех хеш-значений для определения потенциального агрегированного хеш-значения, подлежащего сравнению с эталонным агрегированным хеш-значением.

Второй подвариант второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, эталонное агрегированное хеш-значение сохранено в реестре, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал

связи с реестром, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включает дополнительные этапы:

- вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

- сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

- вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

- получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

- указания результата операции проверки сканером.

Данный второй подвариант второго варианта способа верификации позволяет независимо проверять аутентичность каждой страницы документа, поскольку

потенциальное хеш-значение корневого узла можно вычислить из данных, считываемых на каждой странице, и сравнить с эталонным агрегированным хеш-значением.

Третий подвариант второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, эталонное агрегированное хеш-значение, предоставленное в распоряжение пользователя, сохранено в памяти сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включает дополнительные этапы:

- вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

- сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

- сканирования на носителе эталонного агрегированного хеш-значения для получения сканированного эталонного агрегированного хеш-значения;

- вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

- проверки того, совпадает ли эталонное агрегированное хеш-значение, сохраненное в памяти сканера, с агрегированным хеш-значением сканирования; и

- указания результата операции проверки сканером.

Данный третий подвариант второго варианта способа верификации позволяет независимо автономно проверять аутентичность каждой страницы документа, поскольку потенциальное хеш-значение корневого узла можно вычислить из данных, считываемых на каждой странице, и сравнить с эталонным агрегированным хеш-значением, сохраненным в памяти сканера.

Настоящее изобретение также относится к альтернативному способу верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее компьютера, которые были сгенерированы согласно вышеупомянутому способу генерирования верифицируемых графических символов на указанном дисплее, в котором компьютер имеет приложение для сканирования, запрограммированное в процессоре, выполненном с возможностью сканирования отображаемых удобочитаемых для человека графических символов и машиночитаемых данных с исправлением ошибок, включающему этапы:

- сканирования отображаемых удобочитаемых для человека графических символов с помощью приложения для сканирования, запущенного в процессоре компьютера, для получения блока сканированных графических данных, представляющего собой цифровое представление сканированных удобочитаемых для человека графических символов;

- сканирования отображаемых машиночитаемых данных с исправлением ошибок и с помощью машиночитаемого декодера приложения для сканирования, запущенного в процессоре компьютера, декодирования сканированных машиночитаемых данных с исправлением ошибок для получения соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок;

- исправления блока сканированных графических данных с помощью кода с исправлением ошибок приложения для сканирования, запущенного в процессоре компьютера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как исправленных удобочитаемых для человека графических символов на дисплее, или

(b) отображения сообщения, указывающего на то, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти компьютера.

Данный альтернативный способ верификации (как «способ верификации отображаемых данных») особенно адаптирован для поддержки возможностей офисного программного обеспечения (например, приложений для обработки текста) по обнаружению мошенничества или ошибок в текстовых документах (например, контрактах, отчетах и т. д.), отображаемых на экране компьютера, которые были сгенерированы на компьютере или загружены в компьютер (например, из внешней памяти, такой как USB-ключ, или через канал связи с внешним сервером, например, с почтовым сервером). Определенное приложение, запущенное на компьютере, фактически выполняет операции, осуществляемые сканером в способе верификации.

Настоящее изобретение дополнительно относится к носителю, маркированному удобочитаемыми для человека графическими символами и машиночитаемым представлением связанных данных с исправлением ошибок согласно вышеупомянутому способу нанесения маркировки, или любому из его первого и второго вариантов, или любому из его первого и второго подвариантов указанного второго варианта. Указанный носитель дополнительно маркирован:

- машиночитаемым представлением хеш-значения субблока согласно первому подварианту второго варианта способа нанесения маркировки, или

- связанным машиночитаемым представлением ключа пути верификации согласно второму подварианту второго варианта способа нанесения маркировки.

Согласно другому аспекту настоящее изобретение относится к сканеру, оснащенному блоком формирования изображения, блоком обработки сканера и дисплеем сканера, при этом блок обработки сканера запрограммирован на запуск сканера, выполненного с возможностью считывания верифицируемых графических данных, маркированных на носителе согласно настоящему изобретению, путем реализации этапов способа верификации, или его второго варианта и третьего подварианта его второго варианта.

Сканер может дополнительно быть оснащен блоком связи сканера, выполненным с возможностью установления связи через канал связи с реестром, при этом блок обработки сканера дополнительно запрограммирован на запуск сканера, выполненного с возможностью получения хеш-значения из реестра, путем реализации этапов способа согласно любому из первого варианта способа верификации или первого подварианта или второго подварианта второго варианта способа верификации.

Наконец, настоящее изобретение также относится к компьютерному программному продукту, выполненному с возможностью, при запуске на компьютере, оснащенном процессором, памятью и дисплеем, реализации этапов альтернативного способа верификации (т. е. указанного «способа верификации

отображаемых данных») для верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее, которые были сгенерированы согласно способу нанесения маркировки.

Далее настоящее изобретение будет описано более полно со ссылкой на прилагаемые чертежи, на которых одинаковые цифры представляют одинаковые элементы на разных фигурах и на которых проиллюстрированы основные аспекты и признаки настоящего изобретения.

Краткое описание чертежей

На **фиг. 1** проиллюстрирован пример носителя, маркированного верифицируемыми графическими символами согласно способу нанесения маркировки настоящего изобретения.

На **фиг. 2** представлена блок-схема, на которой проиллюстрирован процесс генерирования и нанесения маркировки в виде верифицируемых графических символов на подложке согласно способу нанесения маркировки настоящего изобретения.

На **фиг. 3** представлена блок-схема процесса генерирования и отображения верифицируемых графических символов на дисплее согласно способу нанесения маркировки настоящего изобретения.

На **фиг. 4** представлена блок-схема, на которой проиллюстрирован процесс генерирования и предоставления верифицируемых графических символов на носителе согласно второму варианту способа нанесения маркировки настоящего изобретения.

На **фиг. 5** показан пример хеш-дерева, используемого во втором подварианте второго варианта способа нанесения маркировки согласно настоящему изобретению.

На **фиг. 6** представлена блок-схема, на которой проиллюстрирован процесс верификации графических символов и машиночитаемых данных, предоставленных на носителе согласно способу верификации настоящего изобретения.

На **фиг. 7** представлена блок-схема, на которой проиллюстрирован вариант осуществления второго варианта способа верификации согласно настоящему изобретению.

Подробное описание

На фиг. 1 проиллюстрирован пример носителя 100, представляющего собой подложку (в данном случае лист бумаги), маркированную удобочитаемым для человека представлением графических символов 110 (в данном случае буквы алфавита, знаки пунктуации и числа, напечатанные на листе 100 бумаги), представляющих собой фрагмент текста контракта, напечатанный в текстовой области 120 носителя 100, вместе с машиночитаемым двухмерным штрих-кодом 130 (в данном случае штрих-код PDF417, т. е. штрих-код «Portable Data File» 417), напечатанный под текстовой областью 120. Фрагмент текста в текстовой области 120 является удобочитаемым для человека представлением соответствующего блока графических данных графических символов.

Двухмерный штрих-код обычно содержит следующие части:

- рисунок локализации (например, форма «L» и линия синхронизации для DataMatrix, или три больших квадрата для QR-кода);

- некоторые информационные поля о формате кода;

- зону данных для хранения данных; а также

- машиночитаемые данные с исправлением ошибок для исправления ошибок считывания (например, данные с исправлением ошибок Рида-Соломона).

Код с исправлением ошибок обычно использует таблицу соответствия, т. е. преобразование между графическими символами заданного конечного набора эталонных графических символов (например, глифов, таких как читаемые символы алфавита) и взаимно однозначными соответствующими кодами (например, символами, закодированными на заданное число m битов).

Штрих-код 130 PDF417 – это хорошо известный многослойный линейный штрих-код (стандарт ISO 15438), который можно считывать с помощью простого линейного сканирования, проводимого по штрих-коду. В варианте осуществления, показанном на фиг. 1, штрих-код 130 PDF417 представляет собой машиночитаемое представление блока данных с исправлением ошибок, который был получен путем применения кода с исправлением ошибок (в данном случае, обычного кода Рида-Соломона) к блоку графических данных расположения графических символов, соответствующих фрагменту текста, показанному в текстовой области 120. Штрих-код 130 PDF417 также содержит (как обычно) данные, относящиеся к версии кода (Рида-Соломона), используемого для вычисления данных с исправлением ошибок, данные, относящиеся к шрифтам, размеру шрифта и межстрочному интервалу текста, числу строк и столбцов текста, относительному местоположению текстовой области относительно маркеров 140, ограничивающих границы блока графических данных (в данном случае, простые метки, указывающие на углы прямоугольной текстовой области 120). Необязательно, штрих-код 130 может дополнительно содержать данные подписи. Эти данные подписи могут быть, например, подписью цифрового представления фрагмента текста с помощью личного ключа шифрования (эта подпись может быть дешифрована с помощью соответствующего открытого ключа).

Фрагмент текста, напечатанный в текстовой области 120, и напечатанный штрих-код 130 PDF417, соответственно, являются примерами удобочитаемых для человека графических символов HrGS и машиночитаемого представления соответствующих данных с исправлением ошибок MrECD, которые были получены посредством способа нанесения маркировки, проиллюстрированного

на фиг. 2. Действительно, на фиг. 2 показана блок-схема процесса генерирования верифицируемых графических данных VGD на подложке (в данном случае листе бумаги) с помощью блока обработки (CPU), который вычисляет блок верифицируемых графических данных VGDB, и нанесения маркировки на подложку с помощью устройства для нанесения маркировки (например, струйного принтера), получившего указанный блок верифицируемых графических данных VGDB. Блок графических данных GDB 210, содержащий цифровое представление графических символов DGS, сохраняют в памяти CPU, при этом каждый графический символ принадлежит заданному конечному набору из M ($M \geq 1$) графических символов {GS(1),…, GS(M)}. Например, конечный набор из M = 26 букв от A до Z английского алфавита. Каждый графический символ GS(i), $i \in \{1,\ldots, M\}$, имеет свое соответствующее цифровое представление DGS(i), и цифровое представление графических символов DGS блока графических данных GDB содержит столько DGS(i), сколько графических символов во фрагменте текста (например, фрагменте текста в текстовой области 120). Процесс генерирования начинается 200 с извлечения 220 цифрового представления графических символов DGS из сохраненного блока графических данных GDB и обработки с помощью запрограммированного кода с исправлением ошибок ECC извлеченного цифрового представления графических символов DGS для получения соответствующих данных с исправлением ошибок ECD. Эти данные с исправлением ошибок ECD представлены в блоке данных с исправлением ошибок ECDB 230. Полученный блок данных с исправлением ошибок ECDB затем форматируют 240 для предоставления соответствующих машиночитаемых данных с исправлением ошибок MrECD, представленных в блоке машиночитаемых данных с исправлением ошибок MrECDB. Блок графических данных GDB также форматируют для получения 215 соответствующего удобочитаемого для человека представления его графических символов HrGS, которые включают в блок данных удобочитаемого для человека графического представления HrGDB. В результате получают 250 блок верифицируемых графических данных VGDB, который состоит из двух соответственных блоков данных: блока данных удобочитаемого для человека

графического представления HrGDB и блока машиночитаемых данных с исправлением ошибок MrECDB. Символически: VGDB = HrGDB + MrECDB. Полученный блок верифицируемых графических данных VGDB затем отправляют на устройство для нанесения маркировки, в данном случае принтер, и их содержимое наносят в виде маркировки 260 (т. е. печатают) на подложку 100 согласно форматированию как соответствующие верифицируемые графические данные VGD. Нанесенные в виде маркировки VGD содержат соответствующие удобочитаемые для человека графические символы HrGS и машиночитаемые данные с исправлением ошибок MrECD (символически: VGD = HrGS + MrECD), которые, соответственно, помещают на лист 100 бумаги согласно форматированию (т. е. как отдельные блоки данных), что говорит о завершении 270 процесса генерирования верифицируемых графических данных на подложке 100 (см. этап (ii) вышеупомянутого способа нанесения маркировки).

Вместо нанесения маркировки на подложку можно отображать фрагмент текста, например, на дисплее планшета или компьютера, как проиллюстрировано на блок-схеме на фиг. 3. Как и на предыдущей фиг. 2, блок графических данных GDB 310, содержащий цифровое представление графических символов DGS, сохраняют в памяти CPU (каждый графический символ принадлежит к заданному конечному набору из $M \geq 1$ графических символов {GS(1),…, GS(M)}). Блок графических данных GDB содержит столько цифровых представлений DGS(i), сколько графических символов GS(i) в отображаемом фрагменте текста. Процесс генерирования начинается 300 с извлечения 320 цифрового представления графических символов DGS из сохраненного блока графических данных GDB и обработки с помощью запрограммированного кода с исправлением ошибок ECC извлеченных DGS для получения соответствующих данных с исправлением ошибок ECD. Эти данные с исправлением ошибок ECD включают в блок данных с исправлением ошибок ECDB 330, который затем форматируют 340 для предоставления соответствующих машиночитаемых данных с исправлением ошибок MrECD, включенных в блок машиночитаемых данных с исправлением ошибок MrECDB. Блок графических данных GDB также

форматируют для получения 315 соответствующего удобочитаемого для человека представления его графических символов HrGS, которые включают в блок данных удобочитаемого для человека графического представления HrGDB. В результате получают 350 блок верифицируемых графических данных VGDB, состоящий из двух соответственных блоков данных HrGDB и MrECDB (символически, VGDB = HrGDB + MrECDB). Блок верифицируемых графических данных VGDB затем отображают 360 на дисплее согласно форматированию как отдельные удобочитаемое для человека представление графических символов HrGS и машиночитаемое представление данных с исправлением ошибок MrECD, что говорит о завершении 370 процесса генерирования верифицируемых графических символов на носителе (см. этап (i) вышеупомянутого способа нанесения маркировки).

Согласно настоящему изобретению несколько вариантов и подвариантов способа нанесения маркировки повышают уровень доверия в соответствии между удобочитаемыми для человека графическими символами, непосредственно считываемыми на носителе пользователем, и удобочитаемой для человека версией, которую можно извлечь из машиночитаемого представления данных с исправлением ошибок (считываемого предназначенным устройством). Эти варианты соответствуют вышеупомянутым первому и второму вариантам.

Первый вариант способа нанесения маркировки использует квази-необратимость односторонних функций, таких как, например, хеш-функции. В этом первом варианте, после осуществления этапов вышеупомянутого способа нанесения маркировки, хеш-функцию H, запрограммированную в блоке обработки, дополнительно используют для получения хеш-значения цифрового представления графических символов или данных с исправлением ошибок (или некоторых частей этих данных), путем вычисления хеш-значения блока графических данных GDB, или блока данных с исправлением ошибок ECDB, или любой части конкатенации (GDB $\oplus$ ECDB) блока графических данных GDB и блока данных с исправлением ошибок ECDB. Хеш-значение (например, с

помощью хеш-функции SHA-256) можно вычислить на основании простого блока графических данных: H(GDB). Предпочтительно, хеш-значение вычисляют на основании блока полной конкатенации: H(GDB ⊕ ECDB). В случае вычисления хеш-значения только на основании части конкатенации блока графических данных GDB и блока данных с исправлением ошибок ECDB, очевидно, что длина в битах этой части должна быть достаточной для обеспечения хорошего уровня безопасности, например, должна по меньшей мере быть равной 100 битам и предпочтительно иметь длину в битах результата, предоставленного выбранной хеш-функцией: например, с помощью хеш-значения SHA-256 длина части в битах составляет по меньшей мере 256 битов (тогда на практике хеш-значение является необратимым). Таким образом, любое изменение, даже одного бита, в аргументе хеш-функции (т. е. любое изменение графических символов или машиночитаемых данных на носителе) приведет к генерированию другого хеш-значения.

В указанном первом варианте способа нанесения маркировки хеш-значение дополнительно сохраняют в реестре, предпочтительно блокчейне (тогда сохраненное значение является практически неизменным), как эталонное хеш-значение H_{ref}. Необязательно, эталонное хеш-значение H_{ref} можно дополнительно подписывать с помощью ключа шифрования, предпочтительно личного ключа Pr_k (сохраненного в памяти блока обработки), для получения соответствующего подписанного эталонного хеш-значения $S(H_{ref})$, и подписанное эталонное хеш-значение $S(H_{ref})$ сохраняют (например, в реестре, таком как база данных или блокчейн) или предоставляют на носителе, эта последняя альтернатива совместима с автономным процессом верификации, при условии что открытый ключ Pu_k, соответствующий личному ключу Pr_k, используют для проверки подписи (например, верификации того, что подписанное эталонное хеш-значение было подписано правильным личным ключом, или даже для извлечения H_{ref} путем дешифрования $S(H_{ref})$ с помощью открытого ключа дешифрования, например, с помощью алгоритма RSA «Ривест-Шамир-Адлеман»).

Второй вариант способа нанесения маркировки, проиллюстрированный вариантом осуществления, показанным на фиг. 4, хорошо подходит для предоставления графических символов на множестве частей носителя, как, например,

- печать (как в случае альтернативы (ii) способа нанесения маркировки) текстового документа, содержащего множество страниц (например, N страниц отчета или контракта и т. д.), или

- отображение (как в случае альтернативы (i) способа нанесения маркировки) цифровой версии текстового документа, состоящего из N страниц, на экране в заданном формате (например, в формате Microsoft Word или pdf), страница за страницей,

при этом каждая из N ($N \geq 2$) страниц, маркированных на подложке, или каждая из N отображаемых страниц показывает определенный фрагмент удобочитаемых для человека графических символов HrGS(j) ($j \in \{1,\ldots,N\}$) и машиночитаемого представления соответствующих данных с исправлением ошибок MrECD(j): оба являются представлениями, полученными из фрагмента верифицируемых графических данных VGD(j) соответствующего определенного субблока верифицируемых графических данных VGDSB(j). В этих случаях согласно указанному второму варианту способа нанесения маркировки способ начинается 400 и (полный) блок графических данных GDB разделяют 410 блоком обработки на N субблоков GDSB(1),…, GDSB(N) (т. е. один субблок для каждой части носителя), при этом каждый субблок графических данных GDSB(j) форматируют для предоставления 415 соответствующего удобочитаемого для человека представления HrGS(j) его графических символов GS(j) в соответствующем субблоке удобочитаемых для человека графических данных HrGDSB(j). Для каждого субблока графических данных GDSB(j) (j=1,…,N) блок обработки генерирует соответствующие данные с исправлением ошибок субблока путем исправления 420 субблока графических данных GDSB (j) с помощью запрограммированного кода с исправлением ошибок ECC, а затем

образует 430 с помощью исправленных данных субблок данных с исправлением ошибок ECDSB(j). Блок обработки генерирует 440 машиночитаемое представление каждого субблока данных с исправлением ошибок ECDSB(j) как соответствующего субблока машиночитаемых данных с исправлением ошибок MrECDSB(j).Блок обработки затем форматирует каждый из субблоков HrGDSB(j) и MrECDSB(j), так что представление последнего на носителе отличается от удобочитаемого для человека представления HrGS(j) графических символов GS(j) первого, для предоставления 450 соответствующего субблока верифицируемых графических данных, символически написанного как VGDSB(j) = HrGDSB(j) + MrECDSB(j). В зависимости от выбранной альтернативы (i) или (ii) способа нанесения маркировки, данные субблоков VGDSB(j), j=1,…,N, отображают 460 на дисплее или наносят в виде маркировки 470 на подложку (например, печатают на листе бумаги, как на фиг. 1) согласно формату как верифицируемые графические данные VGD(j) (символически: VGD(j) = HrGS(j) + MrECD(j)), причем каждую маркировку M(j) VGD(j) предоставляют на части j подложки (например, печатают на j-ой странице документа, состоящего из N страниц), что говорит о завершении 480-490 процесса генерирования верифицируемых графических данных на носителе.

Несколько подвариантов вышеупомянутого второго варианта способа нанесения маркировки повышают уровень доверия в аутентичности удобочитаемых для человека графических символов или машиночитаемого представления данных с исправлением ошибок, предоставленных на носителе. Эти подварианты фактически являются первым и вторым подвариантами. Эти подварианты также используют квази-необратимость односторонних функций (например, хеш-функций, таких как хеш-функции SHA-256). В этих двух подвариантах, после осуществления этапов вышеупомянутого второго варианта способа нанесения маркировки, хеш-функцию H, запрограммированную в блоке обработки, дополнительно используют для получения хеш-значения цифрового представления графических символов или данных с исправлением ошибок (или некоторых частей этих данных). В связи с тем, что в указанном втором варианте способа нанесения маркировки блок графических данных GDB и

соответствующий блок данных с исправлением ошибок ECDB разделяют на N субблоков (соответствующих N частям носителя), существует несколько возможностей для определения для каждого субблока j (j=1,…,N) соответствующего хеш-значения субблока H(j), как объясняется выше: следует выбрать одну из этих возможностей, которая будет служить для вычисления N хеш-значений субблока в любом из этих подвариантов (а также в вариантах способа верификации).

В первом подварианте второго варианта способа нанесения маркировки блок обработки вычисляет для каждого субблока графических данных GDSB(j) (j=1,…,N) хеш-значение субблока H(j): например, в предпочтительном варианте осуществления полную конкатенацию субблока графических данных GDSB(j) и субблока данных с исправлением ошибок ECDSB(j) выбирают для хеш-значения субблока, т. е. H(j) = H(GDSB(j) ⊕ ECDSB(j)). В целом, хеш-значения субблока H(j), j=1,…,N, определяют согласно одной из следующих возможностей: можно иметь H(j) = H(GDSB(j)), или H(j) = H(ECDSB(j)), или взяв хеш-значение любой части конкатенации (GDSB(j) ⊕ ECDSB(j)) субблока графических данных GDSB(j) и субблока данных с исправлением ошибок ECDSB (j), т. е. где H(j) = H(часть (GDSB(j) ⊕ ECDSB(j)) (с ограничением относительно длины в битах уже упомянутой части).

Затем, машиночитаемое представление MrH(j) каждого хеш-значения субблока H(j) вычисляют блоком обработки и связывают с соответствующим субблоком верифицируемых графических данных VGDSB(j) (j=1,…,N). В результате, в дополнение к удобочитаемому для человека представлению j-ых графических символов субблока HrGS(j) и машиночитаемому представлению j-ых данных с исправлением ошибок субблока MrECD(j) (из субблока верифицируемых графических данных VGDSB(j)), j-ая страница документа дополнительно содержит машиночитаемое представление MrH(j) j-ого хеш-значения субблока. Этот подвариант позволяет дополнительно защитить графические данные субблока и соответствующие данные с исправлением ошибок субблока с помощью односторонней хеш-функции, поскольку любое изменение указанных

j-ых данных субблока не позволит извлекать содержимое данных MrH(j). Более того, это дополнительное преимущество достигается с помощью только ограниченных дополнительных данных, предоставленных на носителе в виде простого машиночитаемого представления хеш-значения субблока. В указанном первом подварианте второго варианта способа нанесения маркировки N хеш-значений субблока H(j) (j=1,…,N) затем используют для вычисления эталонного агрегированного хеш-значения H_{ref}. Как упомянуто выше, N хеш-значений субблока H(j), j = 1,…,N, можно вычислить на основании простых субблоков графических данных, т. е. H(j) ≡ H(GDSB(j)). Предпочтительно, хеш-значения субблока вычисляют на основании полной конкатенации субблоков: H(j) ≡ H(GDSB(j) ⊕ ECDSB(j)). Таким образом, любое изменение, даже одного бита, в аргументе любой из хеш-функций субблока H(j) (т. е. любое изменение в графических или машиночитаемых данных субблоков на носителе) будет генерировать разное значение агрегированного хеш-значения H_{ref}. В этом первом подварианте блок обработки конкатенирует все N хеш-значений субблока H(j), j=1,…,N, для получения эталонного агрегированного хеш-значения H_{ref} = H(1) ⊕ H(2) ⊕ … ⊕ H(N-1) ⊕ H(N) (символ ⊕ указывает на операцию конкатенации). Это эталонное хеш-значение H_{ref} дополнительно сохраняют в реестре (т. е. в сервере или базе данных, предпочтительно в блокчейне).

Необязательно, память блока обработки может дополнительно сохранять ключ для шифрования цифровых данных, предпочтительно личный ключ Pr_k в паре с открытым ключом Pu_k (т. е. для шифрования с асимметричным ключом), блок обработки, после конкатенации всех N хеш-значений субблока для получения эталонного агрегированного хеш-значения H_{ref} = H(1) ⊕ H(2) ⊕ … ⊕ H(N-1) ⊕ H(N), может дополнительно подписывать (т. е. шифровать) эталонное агрегированное хеш-значение H_{ref} с помощью ключа шифрования (предпочтительно личного ключа Pr_k) для получения подписи эталонного агрегированного хеш-значения $S(H_{ref})$. Затем эту подпись можно сохранять (например, в памяти блока обработки, или в базе данных, или в блокчейне) или дополнительно предоставлять на носителе. Эта последняя альтернатива

позволяет выполнять автономный процесс верификации, при условии что соответствующий ключ, предпочтительно открытый ключ Pu_k, связанный с личным ключом Pr_k, используют для проверки подлинности подписи (т. е. что она была получена с помощью правильного личного ключа Pr_k).

Во втором подварианте второго варианта способа нанесения маркировки, после вычисления N хеш-значений субблока H(j), j=1,…,N (так же, как в вышеупомянутом первом подварианте), эталонное агрегированное хеш-значение H_{ref} вычисляют блоком обработки как значение корневого узла R дерева, предпочтительно двоичного дерева. Это дерево имеет N хеш-значений субблока H(1), H(2),…, H(N-1), H(N) как листовых узлов, как проиллюстрировано на фиг. 5 (с примером простого двоичного дерева с N = 8). В данном случае также хеш-значения представляют значения, обычно получаемые с помощью односторонней функции (например, хеш-функции H() семейства SHA-256). Таким образом, дерево, как правило, основано на множестве вычисленных хеш-значений субблока H(j), j=1,…,N, и содержит узлы, расположенные согласно заданной упорядоченности узлов в дереве. Дерево содержит уровни узлов, начиная от листовых узлов a(1,j), j=1,…,N, соответственно, соответствующих множеству хеш-значений субблока H(1), H(2),…, H(N-1), H(N), и узлов, отличных от листовых, до корневого узла R дерева, причем каждый узел, отличный от листового (т. е. узел, содержащийся между листовым узлом и корневым узлом), дерева, соответствует хеш-значению конкатенации соответственных хеш-значений его дочерних узлов согласно упорядоченности конкатенации дерева, корневой узел R соответствует эталонному агрегированному хеш-значению H_{ref}, т. е. хеш-значению конкатенации хеш-значений узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева. В примере на фиг. 5, где N = 8, таким образом, имеют восемь листовых узлов (первый уровень дерева) a(1,j) = H(j), j=1,…,8, и для четырех значений узлов второго уровня: a(2,1) = H(a(1,1) $\oplus$ a(1,2)); a(2,2) = H(a(1,3) $\oplus$ a(1,4)); a(2,3) = H(a(1,5) $\oplus$ a(1,6)); a(2,4) = H(a(1,7) $\oplus$ a(1,8)). Для двух значений узлов третьего (предпоследнего) уровня: a(3,1) =

H(a(2,1) ⊕ a(2,2)) и a(3,2) = H(a(2,3) ⊕ a(2,4)). Таким образом, значение корневого узла R: R = H(a(3,1) ⊕ a(3,2)) ≡ H_{ref}.

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

Затем блок обработки вычисляет для каждого хеш-значения субблока H(j) (т. е. для каждого листового узла дерева a(1,j)), j=1,…,N, связанный ключ пути верификации субблока VPK(j). Ключ пути верификации субблока VPK(j), относящийся к листовому узлу a(1,j) (и, таким образом, к хеш-значению субблока H(j)), представляет собой ряд хеш-значений выбранных узлов, отличных от листовых, дерева, которые необходимы для извлечения значения корневого узла R, начиная от листового узла a(1,j). Выбранные узлы, отличные от листовых, фактически соответствуют определенному пути в дереве между листовым узлом a(1,j) и корневым узлом R. Ключ пути верификации субблока, связанный с заданным листовым узлом дерева, фактически представляет собой последовательность соответственных значений узлов, начиная от уровня листовых узлов до предпоследнего уровня узлов, каждого другого листового узла, имеющего такой же родительский узел в дереве, что и заданный листовой узел, и последовательно на каждом следующем уровне в дереве, каждого узла, отличного от листового, имеющего такой же родительский узел в дереве, что и предыдущий такой же родительский узел, рассмотренный на предшествующем уровне. В примере простого двоичного дерева с восемью листовыми узлами a(1,1),…, a(1,8), показанном на фиг. 5, восемь ключей пути верификации субблока VPK(1),…, VPK(8) определяют следующим образом (согласно вышеупомянутому определению):

1) для заданного листового узла a(1,1) = H(1), связанный ключ пути верификации субблока представляет собой VPK(1) = {a(1,2),a(2,2),a(3,2)}, из которого можно извлечь значение корневой цифровой подписи R посредством

следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из заданного листового узла a(1,1) = H(1) и листового узла a(1,2) = H(2) в VPK(1) (a(1,2) представляет собой «другой листовой узел, имеющий такой же родительский узел», т. е. узел a(2,1), «что и заданный листовой узел», т. е. узел a(1,1)), получают значение родительского узла a(2,1) посредством a(2,1) = H(a(1,1) ⊕ a(1,2)) (т. е. a(2,1) = H(H(1) ⊕ H(2))),

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

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

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

Таким образом, на основании VPK(1) = {a(1,2),a(2,2),a(3,2)}, связанного с a(1,1), значение корневого узла дерева можно получить следующим образом: R = H(H(H(a(1,1) ⊕ a(1,2)) ⊕ a(2,2)) ⊕ a(3,2)).

2) для заданного листового узла a(1,2) = H(2), связанный ключ пути верификации субблока представляет собой VPK(2) = {a(1,1),a(2,2),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов

(выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из заданного a(1,2) = H(2) и a(1,1) = H(1) в VPK(2) (a(1,1) представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел a(2,1), что и заданный листовой узел, т. е. узел a(1,2)), получают значение родительского узла a(2,1) посредством a(2,1) = H(a(1,1) ⊕ a(1,2)),

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

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

Таким образом, на основании VPK(2) = {a(1,1),a(2,2),a(3,2)}, связанного с a(1,2), значение корневого узла дерева можно получить следующим образом: R = H(H(H(a(1,1) ⊕ a(1,2)) ⊕ a(2,2)) ⊕ a(3,2)).

3) для заданного листового узла a(1,3) = H(3), ключ пути верификации субблока представляет собой VPK(3) = {a(1,4),a(2,1),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,3) = H(3) и a(1,4) = H(4) в VPK(3) (a(1,4) представляет собой другой листовой узел, имеющий такой же родительский узел, т. е. узел a(2,2), что и

заданный листовой узел, т. е. узел a(1,3)), получают значение родительского узла a(2,2) посредством a(2,2) = H(a(1,3) ⊕ a(1,4)),

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

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

Таким образом, значение корневого узла дерева можно получить как: R = H(H(a(2,1) ⊕ H(a(1,3) ⊕ a(1,4))) ⊕ a(3,2)).

4) для заданного листового узла a(1,4) = H(4), ключ пути верификации субблока представляет собой VPK(4) = {a(1,3),a(2,1),a(3,2)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,4) = H(4) и a(1,3) = H(3) в VPK(4), получают значение родительского узла a(2,2) посредством a(2,2) = H(a(1,3) ⊕ a(1,4)),

ii) из полученного a(2,2) и значения следующего узла в VPK(4), т. е. a(2,1) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,1) посредством a(3,1) = H(a(2,1) ⊕ a(2,2)),

iii) из полученного a(3,1) и значения следующего узла в VPK(4), т. е. a(3,2) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(H(a(2,1) ⊕ H(a(1,3) ⊕ a(1,4))) ⊕ a(3,2)).

5) для заданного узла a(1,5) = H(5), ключ пути верификации субблока представляет собой VPK(5) = {a(1,6),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,5) = H(5) и a(1,6) = H(6) в VPK(5), получают значение родительского узла a(2,3) посредством a(2,3) = H(a(1,5) ⊕ a(1,6)),

ii) из полученного a(2,3) и значения следующего узла в VPK(5), т. е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(5), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(H(a(1,5) ⊕ a(1,6)) ⊕ a(2,4))).

6) для заданного узла a(1,6) = H(6), ключ пути верификации субблока представляет собой VPK(6) = {a(1,5),a(2,4),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,6) = H(6) и a(1,5) = H(5) в VPK(6), получают значение родительского узла a(2,3) посредством a(2,3) = H(a(1,5) ⊕ a(1,6)),

ii) из полученного a(2,3) и значения следующего узла в VPK(6), т. е. a(2,4) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(6), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(H(a(1,5) ⊕ a(1,6)) ⊕ a(2,4))).

7) для заданного узла a(1,7) = H(7), ключ пути верификации субблока представляет собой VPK(7) = {a(1,8),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,7) = H(7) и a(1,8) = H(8) в VPK(7), получают значение родительского узла a(2,4) посредством a(2,4) = H(a(1,7) ⊕ a(1,8)),

ii) из полученного a(2,4) и значения следующего узла в VPK(7), т. е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(7), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(a(2,3) ⊕ H(a(1,7) ⊕ a(1,8)))).

8) для заданного узла a(1,8) = H(8), ключ пути верификации субблока представляет собой VPK(8) = {a(1,7),a(2,3),a(3,1)}, из которого можно извлечь корневое значение R посредством следующих этапов (выполняемых согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева):

i) из a(1,8) = H(8) и a(1,7) = H(7) в VPK(8), получают значение родительского узла a(2,4) посредством a(2,4) = H(a(1,7) ⊕ a(1,8)),

ii) из полученного a(2,4) и значения следующего узла в VPK(8), т. е. a(2,3) следующего уровня узлов, отличных от листовых, получают значение родительского узла a(3,2) посредством a(3,2) = H(a(2,3) ⊕ a(2,4)),

iii) из полученного a(3,2) и значения следующего узла в VPK(8), т. е. a(3,1) предпоследнего уровня узлов, получают значение корневого узла R посредством R = H(a(3,1) ⊕ a(3,2)).

Таким образом, значение корневого узла дерева можно получить как: R = H(a(3,1) ⊕ H(a(2,3) ⊕ H(a(1,7) ⊕ a(1,8)))).

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

- извлечения из последовательности значений узлов в ключе пути верификации субблока значения каждого другого листового узла дерева, имеющего такой же родительский узел, что и у заданного листового узла, и вычисления хеш-значения конкатенации заданного значения узла и, соответственно, согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, извлеченного значения указанного каждого другого листового узла, тем самым получая хеш-значение указанного такого же родительского узла заданного листового узла;

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

.извлечения из последовательности значений узлов в ключе пути верификации субблока значения каждого другого узла, отличного от листового, дерева,

имеющего такой же родительский узел, что и у предыдущего такого же родительского узла, рассмотренного на предшествующем этапе, и

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

- вычисления хеш-значения конкатенации полученных значений узлов, отличных от листовых, соответствующих предпоследнему уровню узлов дерева согласно упорядоченности узлов в дереве и упорядоченности конкатенации дерева, тем самым получая значение корневого узла дерева.

На следующем этапе второго подварианта второго варианта способа нанесения маркировки блок обработки генерирует машиночитаемое представление MrVPK(j) каждого ключа пути верификации субблока VPK(j) (j=1,…,N) и включает его одновременно с соответственно соответствующим субблоком удобочитаемых для человека графических данных HrGDSB(j) и субблоком машиночитаемых данных с исправлением ошибок MrECDSB(j) в субблок верифицируемых графических данных VGDSB(j). Субблок верифицируемых графических данных VGDSB(j) затем дополнительно форматируют для предоставления машиночитаемого представления указанного ключа пути верификации субблока, которое является отдельным от удобочитаемого для человека представления связанного субблока графических данных GDSB(j) и машиночитаемого представления связанного субблока данных с исправлением ошибок ECDSB(j), а затем предоставляют на носителе (как компонент соответствующих верифицируемых графических данных субблока). Таким образом, субблок верифицируемых графических данных теперь символически записывается: VGDSB(j) = HrGDSB(j) + MrECDSB(j) + MrVPK(j), j = 1,…,N. Наконец, далее осуществляют один из следующих этапов:

(iii) эталонное агрегированное хеш-значение H_{ref} = R сохраняют в реестре (предпочтительно в блокчейне),

или

(iv) эталонное агрегированное хеш-значение H_{ref} = R предоставляют в распоряжение пользователю.

Необязательно, H_{ref} можно подписывать с помощью личного ключа подписи Pr_k (сохраненного в памяти блока обработки) блоком обработки для получения подписи эталонного агрегированного хеш-значения $S(H_{ref})$, и подпись эталонного агрегированного хеш-значения $S(H_{ref})$ сохраняют (например, в реестре) или дополнительно предоставляют на носителе или в распоряжение пользователю. Затем, путем использования соответствующего открытого ключа Pu_k возможно проверить, является ли $S(H_{ref})$ подлинной.

В результате для каждого субблока графических данных GDSB(j) (j=1,…,N) блока графических данных GDB на носителе предоставлены соответствующие удобочитаемые для человека графические символы субблока вместе с соответствующими машиночитаемыми данными с исправлением ошибок субблока, которые аутентифицируются пользователем путем извлечения корневого значения R с помощью хеш-значения субблока H(j) и его соответствующего ключа пути верификации VPK(j), которые можно получить из данных, считываемых на носителе, соответственно, из удобочитаемых для человека графических символов субблока HrGS(j) и машиночитаемого представления ключа пути верификации субблока MrVPK(j).

Как ясно из вышеупомянутого примера, значение корневого узла R можно наконец извлечь из любого заданного значения листового узла путем вычисления хеш-значения конкатенации этого заданного значения листового узла только со значениями узлов, определенными в соответствующем ключе пути верификации субблока. Таким образом, объем данных в информации о верификации на основании ключа пути верификации (считываемого на

носителе), который необходим для извлечения значения корневого узла R, явно намного меньше, чем объем данных, необходимый для вычисления эталонного значения корневого узла H_{ref} на основании только всех значений листовых узлов (т. е. путем вычисления всех значений узлов, отличных от листовых, промежуточных уровней дерева): это является преимуществом настоящего изобретения с учетом ограничения ограниченного размера, доступного на машиночитаемом представлении данных (таком как, например, двухмерный штрих-код).

Таким образом, согласно настоящему изобретению переплетение хеш-значений всех оригинальных хеш-значений субблока, благодаря структуре дерева и использованию надежных односторонних функций для вычисления значений узлов дерева (таких как хеш-функции SHA-256 в вышеупомянутом варианте осуществления), вместе со значением корневого узла R дерева (которое может стать неизменным при сохранении в блокчейне), и включение машиночитаемых данных с исправлением ошибок и связанного машиночитаемого ключа пути верификации на носитель вместе с соответствующим удобочитаемым для человека представлением графических данных позволяют предотвращать фальсификацию данных на маркированном носителе с очень высоким уровнем надежности.

Вышеупомянутые варианты осуществления способа нанесения маркировки предоставляют на носителе (листе 100 бумаги или дисплее) удобочитаемые для человека графические символы вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые могут легко верифицироваться пользователем. Действительно, согласно способу верификации настоящего изобретения, иллюстративная блок-схема которого показана на фиг. 6, пользователь с помощью сканера, оснащенного блоком формирования изображения, блоком обработки сканера с памятью сканера, и дисплеем сканера, может проверить, были ли изменены удобочитаемые для человека графические символы HrGS на носителе или нет относительно оригинальных данных, или может даже извлечь оригинальные графические символы. В следующем

иллюстративном варианте осуществления способа верификации удобочитаемые для человека графические символы HrGS составляют текст, предоставленный на носитель согласно способу нанесения маркировки. Например, текст может быть напечатан на подложке (например, листе бумаги, как на фиг. 1) или отображен в электронном виде на экране. Блок формирования изображения сканера выполнен с возможностью отображения текста и соответствующего машиночитаемого представления данных с исправлением ошибок MrECD на носителе. Блок обработки сканера запрограммирован на осуществление обработки изображения носителя, взятого блоком формирования изображения, для извлечения текстовых данных и получения цифрового представления извлеченных текстовых данных как соответствующего блока сканированных графических данных SGDB. Блок обработки сканера также запрограммирован на осуществление обработки изображения машиночитаемого представления данных с исправлением ошибок MrECD на носителе, взятого блоком формирования изображения, для извлечения соответствующих сканированных данных с исправлением ошибок SECD, путем дополнительного использования запрограммированного (в блоке обработки сканера) машиночитаемого декодера, и получения цифрового представления сканированных данных с исправлением ошибок SECD как соответствующего блока сканированных данных с исправлением ошибок SECDB. Блок обработки сканера дополнительно запрограммирован на осуществление операций исправления ошибок блоков данных путем использования кода с исправлением ошибок ECC. Сканер может быть, например, простым смартфоном с камерой (как блоком формирования изображения) и приложениями для обработки изображения, декодирования и исправления ошибок, выполненными с возможностью запуска на его блоке обработки.

Общий процесс верификации, показанный на фиг. 6, с примером маркированного носителя на фиг. 1, начинается 600 путем:

- сканирования (через блок формирования изображения сканера) сканером текста HrGS 610 на носителе, т. е. текста 110 на текстовой области 120 листа 100

бумаги, и получения соответствующего блока сканированных графических данных SGDB 620 (т. е. цифрового представления сканированного текста); или

- сканирования машиночитаемого представления данных с исправлением ошибок MrECD 615 на носителе сканером, т. е. штрих-кода PDF417 130 на листе 100 бумаги, декодирования машиночитаемого представления данных с исправлением ошибок MrECD (с помощью запрограммированного машиночитаемого декодера) для извлечения соответствующих сканированных данных с исправлением ошибок SECD, и образования соответствующего блока сканированных данных с исправлением ошибок SECDB 625 (т. е. цифрового представления извлеченных SECD); и

- исправления 630 блока сканированных графических данных SGDB с помощью кода с исправлением ошибок ECC, запрограммированного в блоке обработки сканера (с использованием извлеченных SECD SECDB), и получения блока исправленных сканированных графических данных CSGDB 640, причем блок исправленных сканированных графических данных CSGDB содержит цифровое представление соответствующих исправленных удобочитаемых для человека графических символов CHrGS; и

- на этапе 650, осуществления по меньшей мере одной из трех альтернатив:

- (a) отображения 660 на дисплее сканера блока исправленных сканированных графических данных CSGDB как соответствующих исправленных удобочитаемых для человека графических символов CHrGS; или

- (b) указания 670 сканером (например, на дисплее сканера, или с помощью любого визуального или звукового сигнала, подаваемого сканером) того, содержит ли блок сканированных графических данных SGDB ошибку (на основании результата исправления 630); или

- (c) сохранения 680 данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных SGDB ошибку (на основании результата исправления 630), в памяти сканера.

Подача результата выбранного(-ых) альтернативы(альтернатив) (a), (b) и (c) приводит к завершению 690 процесса верификации.

Альтернатива (a) позволяет пользователю визуально сравнивать версию текста CHrGS, отображаемую на дисплее сканера, которая была исправлена с помощью запрограммированного кода с исправлением ошибок ECC, с использованием сканированных данных с исправлением ошибок SECD (полученных из машиночитаемого представления данных с исправлением ошибок MrECD), и (неисправленный) текст HrGS, сканированный на носителе. Предпочтительно, различие(-я) отображаемого текста со сканированным текстом можно выделять, чтобы помочь пользователю легко обнаружить и найти любое изменение в тексте (например, из-за изменения или мошенничества).

С помощью альтернативы (b) пользователь может быть предупрежден в случае любого различия между исправленным текстом CHrGS и текстом HrGS, сканированным на носителе.

Альтернатива (c) позволяет отслеживать любые существующие различия между исправленным текстом и текстом, сканированным на носителе. В качестве альтернативы, если сканер дополнительно оснащен средствами связи (например, смартфоном) и может быть подключен к внешнему серверу, данные результата сканирования можно сохранить в памяти сервера через канал связи.

Преимущество вышеупомянутого способа верификации заключается в том, что он позволяет автономно (т. е. без подключения к внешнему устройству через канал связи) проверить соответствие между текстом, предоставленным на носителе, как удобочитаемыми для человека графическими символами, и удобочитаемой для человека версией, которую можно получить из машиночитаемого представления данных с исправлением ошибок, считываемого на носителе: поскольку указанная версия является результатом исправления с помощью кода с исправлением ошибок (аналогично тому, как он уже использовался со способом нанесения маркировки для определения данных с исправлением ошибок, соответствующих тексту, предоставленному на носителе)

текста, считываемого сканером на носителе путем использования данных с исправлением ошибок, извлеченных из машиночитаемого представления, считываемого на носителе, и декодированных, посредством сканера. Однако, в случае если сканер дополнительно оснащен средствами связи (например, смартфоном) и может быть подключен к внешнему серверу, некоторые или все вышеупомянутые операции способа верификации декодирования и выполнения исправления ошибок блока данных можно осуществлять на (предназначенном) внешнем сервере.

Несколько вариантов способа верификации (соответственно коррелированных с первым и вторым вариантами способа нанесения маркировки, используемого для получения верифицируемых графических данных на носителе) позволяют пользователю выходить за пределы простой верификации текста (или, в более общем смысле, графических символов), предоставленного на носителе, путем дополнительной проверки аутентичности текста (и/или машиночитаемых данных).

В первом варианте способа верификации удобочитаемых для человека графических символов HrGS и машиночитаемого представления данных с исправлением ошибок, предоставленных на носителе согласно первому варианту способа нанесения маркировки, после осуществления этапов указанного способа верификации (см. фиг. 6), хеш-функция H дополнительно запрограммирована в блоке обработки сканера для вычисления хеш-значения блока данных (так же, как соответственно указано в первом варианте способа нанесения маркировки), сканер дополнительно подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, при этом эталонное хеш-значение H_{ref} сохраняют (как указано в первом варианте способа нанесения маркировки), и блок обработки сканера дополнительно вычисляет с помощью запрограммированной хеш-функции H хеш-значение сканирования H_{scan} как хеш-значение H(CSGDB) блока исправленных сканированных графических данных CSGDB, или хеш-значение H(SECDB) блока сканированных данных с исправлением ошибок SECDB, или хеш-значение

H(части CDB) любой части блока данных CDB ≡ (CSGDB ⊕ SECDB), полученной в результате конкатенации (CSGDB ⊕ SECDB) блока исправленных сканированных графических данных CSGDB и блока сканированных данных с исправлением ошибок SECDB (как объясняется выше).

Сканер дополнительно осуществляет следующие операции:

- сканер получает через свой блок связи (путем отправки запроса в реестр по каналу связи и приема ответа) эталонное хеш-значение H_{ref}, сохраненное в реестре, и

- затем блок обработки сканера проверяет, совпадает ли полученное эталонное хеш-значение H_{ref} с хеш-значением сканирования H_{scan}; и осуществляет по меньшей мере одну из операций:

(e) он указывает на результат операции проверки (например, через дисплей сканера), или

(f) он сохраняет результат операции проверки в памяти сканера.

Любое изменение относительно оригинального (подлинного) текста (как удобочитаемых для человека графических символов) удобочитаемого для человека текста, предоставленного на носителе, или содержимого его машиночитаемых данных с исправлением ошибок, предоставленных на носителе, будет генерировать несоответствие между эталонным хеш-значением H_{ref} и хеш-значением сканирования H_{scan}. Таким образом, этот вариант повышает уровень доверия к соответствию текста на носителе его оригинальной версии.

Второй вариант способа верификации, проиллюстрированный вариантом осуществления, показанным на фиг. 7, хорошо подходит в случае разделения полного набора графических символов на множество N подмножеств (где $N \geq 2$), причем каждое подмножество графических символов маркировано на соответствующей части подложки, как, например, текст, напечатанный (согласно альтернативе (ii) второго варианта способа нанесения маркировки) на

множестве страниц (например, N страниц отчета или контракта и т. д.), или отображаемый (согласно альтернативе (i) второго варианта способа нанесения маркировки) на экране в заданном формате (например, текстовый документ, состоящий из N страниц, в формате Microsoft Word или pdf), страница за страницей, при этом каждая маркированная часть подложки или каждая отображаемая страница демонстрирует определенное подмножество удобочитаемых для человека графических символов и машиночитаемого представления соответствующих данных с исправлением ошибок (оба являются представлениями, полученными из соответствующего определенного субблока верифицируемых графических данных).

В следующем иллюстративном варианте осуществления второго варианта способа верификации (см. фиг. 7) удобочитаемые для человека графические символы HrGS составляют текст, который предоставлен на носителе согласно второму варианту способа нанесения маркировки. Например, текст может быть напечатан на подложке (например, листе бумаги, как на фиг. 1) или отображен в электронном виде на экране. Блок формирования изображения сканера выполнен с возможностью формирования изображения каждой страницы из N страниц текста на носителе, т. е. каждых из (верифицируемых) удобочитаемых для человека графических символов HrGS(j) и машиночитаемого представления соответствующих данных с исправлением ошибок MrECD(j), предоставленных на j-ой странице (j = 1,…,N). Блок обработки сканера запрограммирован на осуществление обработки изображения j-ой страницы (j = 1,…,N) на носителе, взятого блоком формирования изображения, для извлечения сканированных текстовых данных из сформированного изображения удобочитаемых для человека графических символов HrGS(j) (т. е. сформированного изображения графических символов j-ого субблока) и получения цифрового представления извлеченных данных как соответствующего субблока сканированных графических данных SGDSB(j). Блок обработки сканера также запрограммирован на осуществление обработки изображения страницы j на носителе, взятого блоком формирования изображения, извлечение сканированных данных с исправлением ошибок SECD(j) из сформированного

изображения машиночитаемого представления данных с исправлением ошибок MrECD(j), путем использования машиночитаемого декодера, запрограммированного в блоке обработки сканера, и получения цифрового представления сканированных данных с исправлением ошибок SECD(j) как соответствующего субблока сканированных данных с исправлением ошибок SECDSB(j). Блок обработки сканера дополнительно запрограммирован на осуществление операций исправления ошибок блоков данных путем использования кода с исправлением ошибок ECC. Сканер может быть простым смартфоном с камерой (как блоком формирования изображения) и приложениями для обработки изображения, декодирования и исправления ошибок, выполненными с возможностью запуска на его блоке обработки.

Согласно вышеупомянутому варианту осуществления (фиг. 7) указанного второго варианта способа верификации, в котором удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок были предоставлены на носителе согласно второму варианту способа нанесения маркировки (как показано на фиг. 4), вышеупомянутый сканер начинает 700 выполнение для каждой страницы j (j= 1,…,N) документа следующих операций:

- сканирования 710 блоком формирования изображения сканера удобочитаемых для человека графических символов HrGS(j), предоставленных на странице j носителя, т. е. текста 110 на текстовой области 120 листа 100 бумаги, и получения 720 соответствующего субблока сканированных графических данных SGDSB(j) (т. е. цифрового представления сканированных удобочитаемых для человека графических символов); и

- сканирования 715 блоком формирования изображения сканера машиночитаемого представления данных с исправлением ошибок MrECD(j), предоставленных на странице j носителя, т. е. штрих-кода PDF417 130 на листе 100 бумаги, декодирования блоком обработки сканера сформированного изображения MrECD(j), с использованием запрограммированного машиночитаемого декодера, извлечения соответствующих сканированных

данных с исправлением ошибок SECD(j) и образования соответствующего субблока сканированных данных с исправлением ошибок SECDSB(j) 725 как цифрового представления сканированных данных с исправлением ошибок SECD(j);

- исправления 730 блоком обработки сканера субблока сканированных графических данных SGDSB (j) путем использования кода с исправлением ошибок ECC, запрограммированного в блоке обработки сканера (и использования извлеченных SECD(j) SECDSB(j)), и получения 740 субблока исправленных сканированных графических данных CSGDSB(j); и

- осуществления 750 по меньшей мере одной из трех альтернатив для каждой страницы j:

- (a) отображения 760 на дисплее сканера визуального представления (т. е. удобочитаемого для человека) субблока исправленных сканированных графических данных CSGDB(j) как соответствующих исправленных удобочитаемых для человека графических символов CGS(j); или

- (b) указания 770 сканером (например, на дисплее сканера, или с помощью любого визуального или звукового сигнала, подаваемого сканером) того, содержит ли субблок сканированных графических данных SGDB(j) ошибку (на основании результата исправления 730); или

- (c) сохранения 780 данных результата сканирования, указывающих на то, содержит ли субблок сканированных графических данных SGDB(j) ошибку (на основании результата исправления 730), в памяти сканера.

Подача результата выбранного(-ых) альтернативы(альтернатив) (a), (b) и (c) приводит к завершению 790 второго варианта процесса верификации каждой страницы документа. Если сканер дополнительно оснащен средствами связи (например, смартфоном) и может быть подключен к внешнему серверу, данные результата сканирования альтернативы (c) можно сохранить в памяти сервера через канал связи.

Настоящее изобретение также включает три подварианта вышеупомянутого второго варианта способа верификации. Во всех этих подвариантах, после осуществления этапов варианта осуществления второго варианта способа верификации, как показано на фиг. 7, односторонняя функция, в данном случае хеш-функция H, дополнительно запрограммирована в блоке обработки сканера для вычисления хеш-значения блока данных (так же, как соответственно указано в вариантах способа нанесения маркировки), и блок обработки сканера дополнительно вычисляет с помощью запрограммированной хеш-функции H N хеш-значений субблока сканирования $H_{scan}(j)$ (j=1,…,N), причем каждое хеш-значение субблока сканирования $H_{scan}(j)$ представляет собой хеш-значение как хеш-значение H(CSGDSB(j)) j-ого субблока исправленных сканированных графических данных CSGDSB(j), или хеш-значение H(SECDSB(j)) j-ого субблока сканированных данных с исправлением ошибок SECDSB(j), или хеш-значение H(часть CDB(j)) любой части блока данных CDB(j) ≡ (CSGDSB(j) ⊕ SECDSB(j)), полученной в результате конкатенации (CSGDSB(j) ⊕ SECDSB(j)) j-ого субблока исправленных сканированных графических данных CSGDB(j) и j-ого субблока сканированных данных с исправлением ошибок SECDSB(j). Использование вычисленных хеш-значений субблока сканирования $H_{scan}(j)$ является определенным в каждом из указанного первого, второго и третьего подвариантов второго варианта способа верификации, как подробно описано ниже.

В варианте осуществления первого подварианта варианта осуществления второго варианта способа верификации, в котором удобочитаемые для человека графические символы HrGS(j) и машиночитаемые данные с исправлением ошибок MrECD(j) на носителе были сгенерированы согласно первому подварианту второго варианта способа нанесения маркировки, хеш-функция и код с исправлением ошибок запрограммированы в блоке обработки сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления хеш-значения субблока H(j) на носителе блоком обработки сканера. Более того, сканер подключен к блоку связи сканера,

выполненному с возможностью установления связи через канал связи с реестром, в котором сохраняют эталонное агрегированное хеш-значение. Сканер вычисляет (см. выше) хеш-значения субблока сканирования $H_{scan}(j)$, $j=1,\ldots,N_{,,}$ в случае если это возможно (т. е. если все HrGS(j) и MrECD(j) являются считываемыми). В случае если невозможно вычислить хеш-значение субблока сканирования для некоторой страницы j, например, поскольку HrGS(j) и MrECD(j) на этой j-ой странице являются не считываемыми, сканер сканирует и декодирует машиночитаемое представление MrH(j) хеш-значения субблока H(j) на этой j-ой странице носителя и получает соответствующее декодированное хеш-значение субблока DH(j): это декодированное хеш-значение субблока затем будет служить как хеш-значение субблока сканирования, т. е. $H_{scan}(j) \equiv DH(j)$, для j-ой страницы. Это машиночитаемое представление j-ого хеш-значения субблока MrH(j) связывают с субблоком верифицируемых графических данных VGDSB(j), что соответствует удобочитаемым для человека графическим символам HrGS(j) и машиночитаемому представлению данных с исправлением ошибок MrECD(j), предоставленных на носителе. В результате, все хеш-значения субблока сканирования, необходимые для вычисления агрегированного хеш-значения для всех страниц носителя, являются доступными (либо как вычисленные хеш-значения сканирования $H_{scan}(j)$, либо как идентифицированные с декодированными хеш-значениями DH(j)).

Блок обработки сканера затем выполняет дополнительные операции:

- вычисления агрегированного хеш-значения сканирования H_{scan} путем конкатенации всех полученных хеш-значений сканирования (символ $\oplus$ представляет собой оператор конкатенации):

$$H_{scan} \equiv H_{scan}(1) \oplus H_{scan}(2) \oplus \ldots \oplus H_{scan}(N-1) \oplus H_{scan}(N).$$

- отправки блоком связи сканера через канал связи запроса на эталонное агрегированное хеш-значение в реестр и приема обратно эталонного агрегированного хеш-значения H_{ref};

- проверки того, совпадает ли принятое эталонное агрегированное хеш-значение H_{ref} с агрегированным значением сканирования H_{scan}, и указания результата операции проверки (например, посредством сообщения на дисплее сканера). В случае совпадения все страницы являются подлинными (т. е. соответствуют оригинальным страницам), даже если текст и машиночитаемые данные с исправлением ошибок на некоторых страницах не могли быть считаны (машиночитаемые представления хеш-значений субблока, однако, являются считываемыми). В случае несовпадения, по меньшей мере одна из страниц была изменена (например, по меньшей мере один из графических символов изменен или подделан): затем возможно извлечь такую страницу путем проверки того, совпадают ли хеш-значения субблока сканирования Hscan(j), полученные из данных субблока HrGS(j) и MrECD(j), с соответствующими декодированными хеш-значениями DH(j), j=1,…,N.

Этот подвариант позволяет независимо проверять сканером, является ли каждая страница документа, состоящая из N страниц, подлинной с помощью сканирования простого машиночитаемого представления хеш-значения субблока ограниченного размера.

В варианте осуществления второго подварианта второго варианта способа верификации удобочитаемые для человека графические символы HrGS(j), (j=1,…,N) и машиночитаемые данные с исправлением ошибок MrECD(j) на странице j (документа, состоящего из N страниц) на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, альтернатива (iii), сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, содержащим эталонное агрегированное хеш-значение H_{ref} (как значение корневого узла дерева, см. фиг. 5), хеш-функцию (такую же, что используется для вычисления N хеш-значений субблока H(j), и соответствующее эталонное агрегированное хеш-значение H_{ref}) запрограммировано в блоке обработки сканера. Сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления MrVPK(j)

(j=1,…,N) ключа пути верификации субблока VPK(j) на носителе и вычисления агрегированного хеш-значения сканирования H_{scan} из пары соответствующего хеш-значения субблока H(j) и ключа пути верификации субблока VPK(j), сканированного на носителе (в данном случае, рассматривают случай, где N = 8, с двоичным деревом, что соответствует примеру на фиг. 5 для документа, состоящего из 8 страниц). После вычисления с помощью хеш-функции (см. выше) хеш-значения субблока сканирования $H_{scan}(j)$, ($j\epsilon\{1,\ldots,N\}$) из сканированных верифицируемых графических данных на странице j документа, состоящего из N страниц, и согласно второму подварианту второго варианта способа нанесения маркировки (т. е. с таким же выбранным выбором H(CSGDSB(j)), или H(SECDSB(j) или H(части CDB(j) для вычисления хеш-значения субблока, используемого как листовые узлы дерева), сканер выполняет дополнительные операции:

- сканирования машиночитаемого представления MrVPK(j) ключа пути верификации субблока VPK(j) на j-ой странице носителя (что соответствует j-ому субблоку исправленных сканированных графических данных CSGDSB(j)) и извлечения соответствующего сканированного ключа пути верификации субблока SVPK(j) блоком обработки сканера;

- вычисления блоком обработки сканера агрегированного хеш-значения сканирования H_{scan} с помощью вычисленного хеш-значения субблока сканирования $H_{scan}(j)$ и сканированного ключа пути верификации субблока SVPK(j), полученного путем сканирования j-ой страницы документа, как объясняется ниже:

.Если j = 1 (первая страница документа), и как объясняется выше касательно варианта осуществления второго подварианта второго варианта способа нанесения маркировки (см. также иллюстративное двоичное дерево на фиг. 5), хеш-значение субблока $H_{scan}(1)$, полученное как указано выше (т. е. из первого субблока исправленных сканированных графических данных CSGDB(1) и/или первого субблока сканированных данных с исправлением ошибок SECDSB(1))

считается значением первого листового узла a(1,1) двоичного дерева (выбирается такая же упорядоченность узлов и упорядоченность конкатенации дерева, что и в вышеупомянутом варианте осуществления второго подварианта второго варианта способа нанесения маркировки), извлеченный сканированный ключ пути верификации субблока SVPK(1) содержит три значения узлов: SVPK(1)={a(1,2),a(2,2),a(3,2)}, таким образом, хеш-значение сканирования H_{scan}, которое можно получить из сканирования верифицируемых графических данных первой страницы, вычисляют следующим образом

$$H_{scan} = H(H(H(a(1,1) \oplus a(1,2)) \oplus a(2,2)) \oplus a(3,2))$$

$$= H(H(H(H_{scan}(1) \oplus a(1,2)) \oplus a(2,2)) \oplus a(3,2))$$

.Если j = 2, где SVPK(2) = {a(1,1), a(2,2), a(3,2)},

$$H_{scan} = H(H(H(a(1,1) \oplus H_{scan}(2)) \oplus a(2,2)) \oplus a(3,2))$$

.Если j = 3, где SVPK(3) = {a(1,4),a(2,1),a(3,2)},

$$H_{scan} = H(H(a(2,1) \oplus H(H_{scan}(3) \oplus a(1,4))) \oplus a(3,2))$$

.Если j = 4, где SVPK(4) = {a(1,3),a(2,1),a(3,2)}

$$H_{scan} = H(H(a(2,1) \oplus H(a(1,3) \oplus H_{scan}(4))) \oplus a(3,2))$$

.Если j = 5, где SVPK(5) = {a(1,6),a(2,4),a(3,1)}

$$H_{scan} = H(a(3,1) \oplus H(H(H_{scan}(5) \oplus a(1,6)) \oplus a(2,4)))$$

.Если j = 6, где SVPK(6) = {a(1,5),a(2,4),a(3,1)}

$$H_{scan} = H(a(3,1) \oplus H(H(a(1,5) \oplus H_{scan}(6)) \oplus a(2,4)))$$

.Если j = 7, где SVPK(7) = {a(1,8),a(2,3),a(3,1)},

$$H_{scan} = H(a(3,1) \oplus H(a(2,3) \oplus H(H_{scan}(7) \oplus a(1,8))))$$

.Если j = 8, где SVPK(8) = {a(1,7),a(2,3),a(3,1)},

$$H_{scan} = H(a(3,1) \oplus H(a(2,3) \oplus H(a(1,7) \oplus H_{scan}(8)))).$$

- далее, получения эталонного агрегированного хеш-значения H_{ref} (т. е. значения корневого узла R дерева), сохраненного в реестре, блоком связи сканера и каналом связи, и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение H_{ref} с агрегированным хеш-значением сканирования H_{scan}, для j=1,…,N; и

- указания результата операции проверки (например, на дисплее сканера).

Этот подвариант способа верификации позволяет обнаруживать любую ошибку на каждой странице документа только с небольшим объемом данных, поскольку любое изменение в содержимом страницы приводит в результате к несовпадению между эталонным агрегированным хеш-значением H_{ref} и хеш-значением сканирования H_{scan}, полученным из верифицируемых графических данных, сканированных на этой странице. Более того, этот способ является надежным, поскольку исправленную версию сканированных графических данных используют для вычисления хеш-значений субблока $H_{scan}(j)$ j-ой страницы, j=1,…,N.

В варианте осуществления третьего подварианта второго варианта способа верификации используют такое же двоичное дерево документа, состоящего из N = 8 страниц, а также такой же способ вычисления хеш-значений субблока сканирования $H_{scan}(j)$ (j=1,…,N) и хеш-значений сканирования H_{scan}, что и в вышеупомянутом примере второго подварианта второго варианта способа верификации. В этом варианте осуществления удобочитаемые для человека графические символы HrGS(j) и машиночитаемые данные с исправлением ошибок MrECD(j) на носителе были сгенерированы согласно второму подварианту второго варианта способа нанесения маркировки, альтернатива (iv), эталонное агрегированное хеш-значение H_{ref} сохраняют в памяти сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования

машиночитаемого представления ключа пути верификации субблока VPK(j) на носителе и вычисления агрегированного хеш-значения $H_{scan}(j)$ из пары соответствующего хеш-значения субблока и ключа пути верификации субблока. Согласно этому варианту осуществления, после осуществления этапов указанного второго варианта способа верификации и вычисления хеш-значения субблока сканирования $H_{scan}(j)$ (j=1,…,N), как упомянуто выше, сканер выполняет дополнительные этапы:

- сканирования сканером машиночитаемого представления MrVPK(j) ключа пути верификации субблока VPK(j) на j-ой странице, предоставленной на носителе (что соответствует j-ому субблоку исправленных сканированных графических данных CSGDSB(j), например, полученному из сканированных верифицируемых графических данных, предоставленных на j-ой странице документа), и извлечения соответствующего сканированного ключа пути верификации субблока SVPK(j) блоком обработки сканера;

- вычисления агрегированного хеш-значения сканирования H_{scan} с помощью вычисленного хеш-значения субблока сканирования $H_{scan}(j)$ и сканированного ключа пути верификации субблока SVPK(j), полученного путем сканирования j-ой страницы документа (см. выше, подробное вычисление, относящееся ко второму подварианту варианта осуществления второго варианта способа верификации);

- получения эталонного агрегированного хеш-значения H_{ref}, сохраненного в памяти сканера;

- проверки блоком обработки сканера того, совпадает ли полученное эталонное агрегированное хеш-значение H_{ref} с агрегированным хеш-значением сканирования H_{scan} для j-ой страницы (j=1,…,N); и

- указания результата операции проверки (через дисплей сканера).

Этот подвариант способа верификации позволяет обнаруживать любую ошибку надежным автономным способом на каждой странице документа только с

небольшим объемом данных, поскольку любое изменение в содержимом страницы приводит в результате к несовпадению между эталонным агрегированным хеш-значением H_{ref} и хеш-значением сканирования H_{scan}, полученным из верифицируемых графических данных, сканированных на этой странице. Действительно, способ только использует данные (ограниченного размера), сохраненные в памяти сканера (т. е. H_{ref}), для проверки того, совпадает ли эталонное агрегированное хеш-значение H_{ref} с хеш-значением сканирования H_{scan}.

Вариант осуществления альтернативного варианта способа верификации иллюстрирует приложение настоящего изобретения для верификации удобочитаемых для человека графических символов и соответствующих машиночитаемых данных с исправлением ошибок, сгенерированных в компьютере, подключенном к дисплею, процессором, запрограммированным на осуществление этапов вышеупомянутого способа нанесения маркировки, альтернатива (i). Компьютер имеет приложение для сканирования, запрограммированное в его процессоре, которое выполнено с возможностью сканирования отображаемых удобочитаемых для человека графических символов и машиночитаемых данных с исправлением ошибок.

Таким образом, компьютер отображает сгенерированные удобочитаемые для человека графические символы HrGS и соответствующие машиночитаемые данные с исправлением ошибок MrECD, и приложение для сканирования, запущенное в процессоре компьютера, затем осуществляет следующие операции:

- сканирования отображаемых удобочитаемых для человека графических символов HrGS для получения блока сканированных графических данных SGDB, причем этот блок сканированных графических данных представляет собой цифровое представление сканированных удобочитаемых для человека графических символов;

- сканирования отображаемых машиночитаемых данных с исправлением ошибок MrECD и с помощью машиночитаемого декодера приложения для сканирования, запущенного в процессоре компьютера, декодирования сканированных машиночитаемых данных с исправлением ошибок MrECD для получения соответствующих сканированных данных с исправлением ошибок SECD в блоке сканированных данных с исправлением ошибок SECDB;

- исправления блока сканированных графических данных SGDB с помощью кода с исправлением ошибок ECC приложения для сканирования, запущенного в процессоре компьютера, с использованием сканированных данных с исправлением ошибок SECD блока сканированных данных с исправлением ошибок SECDB для получения соответствующего блока исправленных сканированных графических данных CSGDB; и

- осуществления по меньшей мере одного из следующих этапов:

(a) отображения визуального представления блока исправленных сканированных графических данных CSGDB как исправленных удобочитаемых для человека графических символов CHrGS на дисплее, или

(b) отображения сообщения, указывающего на то, содержит ли блок сканированных графических данных SGDB ошибку (на основании результата этапа исправления SGDB), или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных SGDB ошибку, в памяти компьютера.

На этапе (a) части первоначально отображаемых удобочитаемых для человека графических символов HrGS (перед запуском приложения для сканирования), которые были исправлены с помощью приложения для сканирования, предпочтительно выделяют для упрощения идентификации и местоположения ошибок в изначально отображаемых HrGS пользователем компьютера.

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

Первоначально поданная формула изобретения

1. Способ генерирования на носителе верифицируемых графических данных с использованием заданного конечного набора графических символов, причем носитель является дисплеем или подложкой, включающий этапы:

сохранения в памяти блока обработки блока графических данных, содержащего цифровое представление графических символов;

обработки блоком обработки цифрового представления графических символов сохраненного блока графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки, для генерирования данных с исправлением ошибок в соответствующем блоке данных с исправлением ошибок;

форматирования блока графических данных и блока данных с исправлением ошибок блоком обработки для предоставления, соответственно, в блоке удобочитаемых для человека графических данных удобочитаемого для человека представления графических символов блока графических данных и в блоке машиночитаемых данных с исправлением ошибок машиночитаемого представления данных с исправлением ошибок блока данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов блока графических данных для получения соответствующего блока верифицируемых графических данных, содержащего указанный блок удобочитаемых для человека графических данных и указанный блок машиночитаемых данных с исправлением ошибок; и

(i) отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок полученного блока верифицируемых графических данных на дисплее, подключенном к блоку обработки, или

(ii) нанесения маркировки на подложку устройством для нанесения маркировки, подключенным к блоку обработки и оснащенным блоком контроля,

выполненным с возможностью контроля операции нанесения маркировки на основании данных, принятых от блока обработки, в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок блока верифицируемых графических данных, принятого от блока обработки,

с предоставлением тем самым на носителе удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые верифицируются пользователем.

2. Способ по п. 1, отличающийся тем, что машиночитаемое представление данных с исправлением ошибок представляет собой любое из буквенно-цифрового представления или представления в виде штрих-кода.

3. Способ по п. 1 или 2, отличающийся тем, что графические символы представляют собой текстовые символы, и конечный набор графических символов представляет собой алфавит.

4. Способ по любому из пп. 1–3, включающий этапы:

вычисления с помощью хеш-функции, запрограммированной в блоке обработки, хеш-значения блока графических данных, или блока данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока графических данных и блока данных с исправлением ошибок; и

сохранения вычисленного хеш-значения как эталонного хеш-значения в реестре.

5. Способ по любому из пп. 1–3, отличающийся тем, что носитель содержит множество частей, и блок верифицируемых графических данных разделяют на одинаковое множество субблоков верифицируемых графических данных, и соответствующие удобочитаемые для человека графические символы и машиночитаемое представление данных с исправлением ошибок, соответственно, распределяют вместе на соответствующие части носителя, посредством следующих этапов, на которых:

блок графических данных разделяют на множество субблоков графических данных, и каждый субблок графических данных форматируют для предоставления удобочитаемого для человека представления его графических символов в соответствующем субблоке удобочитаемых для человека графических данных;

для каждого субблока графических данных цифровое представление его графических символов извлекают и обрабатывают с помощью кода с исправлением ошибок для генерирования соответствующих данных с исправлением ошибок в субблоке данных с исправлением ошибок;

каждый субблок данных с исправлением ошибок форматируют для предоставления в соответствующем субблоке машиночитаемых данных с исправлением ошибок машиночитаемого представления соответствующих данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов соответствующего субблока удобочитаемых для человека графических данных для получения соответствующего субблока верифицируемых графических данных, содержащего указанный субблок удобочитаемых для человека графических данных и указанный субблок машиночитаемых данных с исправлением ошибок; и

на этапе (i), отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок каждого полученного субблока верифицируемых графических данных на дисплее, или

на этапе (ii), нанесения маркировки на подложку устройством для нанесения маркировки в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок каждого субблока верифицируемых графических данных, принятого блоком контроля от блока обработки,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые верифицируются пользователем.

6. Способ по п. 5, отличающийся тем, что

хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

для каждого хеш-значения субблока вычисляют соответствующее машиночитаемое представление указанного хеш-значения субблока;

одновременно с каждым субблоком верифицируемых графических данных, соответствующее машиночитаемое представление хеш-значения субблока дополнительно предоставляют на соответствующей части носителя;

эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как конкатенацию всех вычисленных хеш-значений субблоков; и

эталонное агрегированное хеш-значение сохраняют в реестре,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

7. Способ по п. 5, отличающийся тем, что

хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических

данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как значение корневого узла дерева, имеющего вычисленные хеш-значения субблоков как значения листовых узлов, причем дерево содержит узлы, расположенные согласно заданной упорядоченности узлов в дереве, указанное дерево содержит уровни узлов, начиная от листовых узлов до корневого узла, причем каждое значение узла, отличного от листового, дерева соответствует хеш-значению конкатенации соответственных значений узлов его дочерних узлов согласно упорядоченности конкатенации дерева, значение корневого узла соответствует хеш-значению конкатенации значений узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

для каждого хеш-значения субблока связанный ключ пути верификации субблока определяют как ряд хеш-значений выбранных узлов, отличных от листовых, дерева, необходимых для извлечения значения корневого узла из указанного хеш-значения субблока;

машиночитаемое представление каждого ключа пути верификации субблока включают, одновременно с соответственно соответствующим субблоком графических данных и субблоком данных с исправлением ошибок, в субблок верифицируемых графических данных, причем субблок верифицируемых графических данных дополнительно форматируют для предоставления машиночитаемого представления указанного ключа пути верификации субблока отдельно от удобочитаемого для человека представления связанного субблока графических данных и машиночитаемого представления связанного субблока данных с исправлением ошибок; и

(iii) эталонное агрегированное хеш-значение сохраняют в реестре, или

(iv) эталонное агрегированное хеш-значение предоставляют в распоряжение пользователя,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

8. Способ верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемым представлением данных с исправлением ошибок на носителе, которые были сгенерированы согласно способу по любому из пп. 1–3, включающий этапы:

сканирования сканером, оснащенным блоком формирования изображения, блоком обработки сканера, имеющим память сканера и подключенным к дисплею сканера, удобочитаемых для человека графических символов на носителе для получения путем обработки изображения сканированных удобочитаемых для человека графических символов блока сканированных графических данных, представляющего собой цифровое представление указанных сканированных удобочитаемых для человека графических символов;

сканирования сканером машиночитаемого представления данных с исправлением ошибок на носителе для получения с помощью машиночитаемого декодера, запрограммированного в блоке обработки сканера, соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок, причем блок сканированных данных с исправлением ошибок представляет собой цифровое представление указанных сканированных данных с исправлением ошибок;

исправления блока сканированных графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки сканера, с использованием сканированных данных с исправлением ошибок блока

сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как соответствующих исправленных удобочитаемых для человека графических символов на дисплее сканера, или

(b) указания сканером того, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти сканера.

9. Способ по п. 8, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 4, причем хеш-функция запрограммирована в блоке обработки сканера, и сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включающий дополнительные этапы:

вычисления по п. 4 с помощью хеш-функции, запрограммированной в блоке обработки сканера, хеш-значения сканирования блока исправленных сканированных графических данных, или блока сканированных данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока исправленных сканированных графических данных и блока сканированных данных с исправлением ошибок;

получения эталонного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное хеш-значение с хеш-значением сканирования; и

(e) указания результата операции проверки, или

(f) сохранения результата операции проверки в

памяти сканера.

10. Способ по п. 8, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 5, при этом:

операция сканирования удобочитаемых для человека графических символов на носителе включает сканирование графических символов соответствующего субблока графических данных для получения путем обработки изображения соответствующего субблока сканированных графических данных как цифрового представления сканированных графических символов субблока;

операция сканирования машиночитаемых данных с исправлением ошибок на носителе включает сканирование данных с исправлением ошибок соответствующего субблока данных с исправлением ошибок для получения соответствующего субблока сканированных данных с исправлением ошибок;

операция исправления блока сканированных графических данных включает исправление графических данных субблока сканированных графических данных с использованием соответствующего субблока сканированных данных с исправлением ошибок для получения соответствующего субблока исправленных сканированных графических данных; и

операция (a) отображения визуального представления блока исправленных сканированных данных включает отображение визуального представления субблока исправленных сканированных графических данных;

операция (b) указания того, содержит ли блок сканированных графических данных ошибку, включает указание того, содержит ли субблок сканированных графических данных ошибку;

операция (c) сохранения данных результата сканирования включает сохранение того, содержит ли субблок сканированных графических данных ошибку.

11. Способ по п. 10, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 6, причем хеш-функция и код с исправлением ошибок запрограммированы в блоке обработки сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления хеш-значения субблока на носителе блоком обработки сканера, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включающий дополнительные этапы:

вычисления для каждой части носителя с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования соответствующего субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока исправленных сканированных графических данных и указанного субблока сканированных данных с исправлением ошибок;

в случае если невозможно вычислить хеш-значение субблока сканирования для части носителя, сканирования и декодирования машиночитаемого представления хеш-значения субблока на указанной части носителя для получения соответствующего декодированного хеш-значения субблока, а также использования этого декодированного хеш-значения субблока как хеш-значения субблока сканирования для этой части носителя;

вычисления агрегированного хеш-значения сканирования как конкатенации всех хеш-значений субблока сканирования;

получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное

эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

указания результата операции проверки сканером.

12. Способ по п. 10, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на каждой части носителя были сгенерированы согласно способу по п. 7, причем эталонное агрегированное хеш-значение сохранено в реестре, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включающий дополнительные этапы:

вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

указания результата операции проверки сканером.

13. Способ по п. 10, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 7, причем эталонное агрегированное хеш-значение, представленное в распоряжение пользователя, сохранено в памяти сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включающий дополнительные этапы:

вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных

сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

сканирования на носителе эталонного агрегированного хеш-значения для получения сканированного эталонного агрегированного хеш-значения;

вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

проверки того, совпадает ли эталонное агрегированное хеш-значение, сохраненное в памяти сканера, с агрегированным хеш-значением сканирования; и

указания результата операции проверки сканером.

14. Способ верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее компьютера, которые были сгенерированы согласно способу по любому из пп. 1–3, причем компьютер имеет приложение для сканирования, запрограммированное в процессоре, выполненном с возможностью сканирования отображаемых удобочитаемых для человека графических символов и машиночитаемых данных с исправлением ошибок, включающий этапы:

сканирования отображаемых удобочитаемых для человека графических символов с помощью приложения для сканирования, запущенного в процессоре компьютера, для получения блока сканированных графических данных, представляющего собой цифровое представление сканированных удобочитаемых для человека графических символов;

сканирования отображаемых машиночитаемых данных с исправлением ошибок и с помощью машиночитаемого декодера приложения для сканирования,

запущенного в процессоре компьютера, декодирования сканированных машиночитаемых данных с исправлением ошибок для получения соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок;

исправления блока сканированных графических данных с помощью кода с исправлением ошибок приложения для сканирования, запущенного в процессоре компьютера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как исправленных удобочитаемых для человека графических символов на дисплее, или

(b) отображения сообщения, указывающего на то, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти компьютера.

15. Носитель, маркированный верифицируемыми графическими данными согласно способу по любому из пп. 1–7.

16. Сканер, оснащенный блоком формирования изображения, блоком обработки сканера и дисплеем сканера, отличающийся тем, что блок обработки сканера запрограммирован на запуск сканера, выполненного с возможностью считывания верифицируемых графических данных, маркированных на носителе по п. 15, путем реализации этапов способа по любому из пп. 8, 10 и 13.

17. Сканер по п. 16, дополнительно оснащенный блоком связи сканера, выполненным с возможностью установления связи через канал связи с реестром, отличающийся тем, что блок обработки сканера дополнительно запрограммирован на запуск сканера, выполненного с возможностью получения

хеш-значения из реестра, путем реализации этапов способа по любому из пп. 9, 11 и 12.

18. Компьютерный программный продукт, выполненный с возможностью, при запуске на компьютере, оснащенном процессором, памятью и дисплеем, реализации этапов способа по п. 14 для верификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее, которые были сгенерированы согласно способу по любому из пп. 1–3.

Формула изобретения, измененная по ст. 34 PCT

1. Способ защиты графических данных от подделки и фальсификации, включающий этапы:

сохранения в памяти блока обработки блока (210, 310) графических данных, содержащего цифровое представление заданного конечного набора графических символов графических данных;

обработки блоком обработки цифрового представления графических символов сохраненного блока графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки, для генерирования данных с исправлением ошибок в соответствующем блоке (230, 330) данных с исправлением ошибок;

форматирования (215, 240; 315, 340) блока графических данных и блока данных с исправлением ошибок блоком обработки для предоставления, соответственно, в блоке удобочитаемых для человека графических данных, удобочитаемого для человека представления графических символов блока графических данных и в блоке машиночитаемых данных с исправлением ошибок машиночитаемого представления данных с исправлением ошибок блока данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов блока графических данных для получения (250, 350) соответствующего блока аутентифицируемых графических данных, содержащего указанный блок удобочитаемых для человека графических данных и указанный блок машиночитаемых данных с исправлением ошибок; и

(i) отображения удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок полученного блока аутентифицируемых графических данных на носителе (100), представляющем собой дисплей, подключенный к блоку обработки, или

(ii) нанесения маркировки (260) на носитель (100), представляющий собой подложку, устройством для нанесения маркировки, подключенным к блоку обработки и оснащенным блоком контроля, выполненным с возможностью контроля операции нанесения маркировки на основании данных, принятых от блока обработки, в виде удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок полученного блока аутентифицируемых графических данных, принятого от блока обработки,

с предоставлением тем самым на носителе данных аутентификации, содержащих удобочитаемые для человека графические символы и соответствующие машиночитаемые данные с исправлением ошибок.

2. Способ по п. 1, отличающийся тем, что машиночитаемое представление данных с исправлением ошибок представляет собой любое из буквенно-цифрового представления или представления в виде штрих-кода (130).

3. Способ по п. 1 или 2, отличающийся тем, что графические символы представляют собой текстовые символы (110), и конечный набор графических символов представляет собой алфавит.

4. Способ по любому из пп. 1–3, включающий этапы:

вычисления с помощью хеш-функции, запрограммированной в блоке обработки, хеш-значения блока графических данных, или блока данных с исправлением ошибок, или любой части блока данных, полученной в результате конкатенации блока графических данных и блока данных с исправлением ошибок; и

сохранения вычисленного хеш-значения как эталонного хеш-значения в реестре.

5. Способ по любому из пп. 1–3, отличающийся тем, что носитель содержит множество частей, и блок аутентифицируемых графических данных разделяют (410) на одинаковое множество субблоков аутентифицируемых графических данных, и соответствующие удобочитаемые для человека графические символы

и машиночитаемое представление данных с исправлением ошибок, соответственно, распределяют вместе на соответствующие части носителя, посредством следующих этапов, на которых:

блок графических данных разделяют на множество субблоков графических данных, и каждый субблок графических данных форматируют (415) для предоставления удобочитаемого для человека представления его графических символов в соответствующем субблоке удобочитаемых для человека графических данных;

для каждого субблока графических данных цифровое представление его графических символов извлекают и обрабатывают (420) с помощью кода с исправлением ошибок для генерирования (430) соответствующих данных с исправлением ошибок в субблоке данных с исправлением ошибок;

каждый субблок данных с исправлением ошибок форматируют для предоставления (440) в соответствующем субблоке машиночитаемых данных с исправлением ошибок машиночитаемого представления соответствующих данных с исправлением ошибок отдельно от удобочитаемого для человека представления графических символов соответствующего субблока удобочитаемых для человека графических данных для получения (450) соответствующего субблока аутентифицируемых графических данных, содержащего указанный субблок удобочитаемых для человека графических данных и указанный субблок машиночитаемых данных с исправлением ошибок; и

на этапе (i), отображения (460) удобочитаемых для человека графических символов и соответствующего машиночитаемого представления данных с исправлением ошибок каждого полученного субблока аутентифицируемых графических данных на дисплее, или

на этапе (ii), нанесения маркировки (470) на подложку устройством для нанесения маркировки в виде удобочитаемых для человека графических

символов и соответствующего машиночитаемого представления данных с исправлением ошибок каждого субблока аутентифицируемых графических данных, принятого блоком контроля от блока обработки,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

6. Способ по п. 5, отличающийся тем, что

хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

для каждого хеш-значения субблока вычисляют соответствующее машиночитаемое представление указанного хеш-значения субблока;

одновременно с каждым субблоком аутентифицируемых графических данных, соответствующее машиночитаемое представление хеш-значения субблока дополнительно предоставляют на соответствующей части носителя;

эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как конкатенацию всех вычисленных хеш-значений субблоков; и

эталонное агрегированное хеш-значение сохраняют в реестре,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

7. Способ по п. 5, отличающийся тем, что

хеш-значение субблока вычисляют с помощью хеш-функции, запрограммированной в блоке обработки, для каждого субблока графических данных, или соответствующего субблока данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока графических данных и указанного субблока данных с исправлением ошибок;

эталонное агрегированное хеш-значение из всех хеш-значений субблоков определяют как значение корневого узла дерева, имеющего вычисленные хеш-значения субблоков как значения листовых узлов, причем дерево содержит узлы, расположенные согласно заданной упорядоченности узлов в дереве, указанное дерево содержит уровни узлов, начиная от листовых узлов до корневого узла, причем каждое значение узла, отличного от листового, дерева соответствует хеш-значению конкатенации соответственных значений узлов его дочерних узлов согласно упорядоченности конкатенации дерева, значение корневого узла соответствует хеш-значению конкатенации значений узлов предпоследнего уровня узлов в дереве согласно указанной упорядоченности конкатенации дерева;

для каждого хеш-значения субблока связанный ключ пути верификации субблока определяют как ряд хеш-значений выбранных узлов, отличных от листовых, дерева, необходимых для извлечения значения корневого узла из указанного хеш-значения субблока;

машиночитаемое представление каждого ключа пути верификации субблока включают, одновременно с соответственно соответствующим субблоком графических данных и субблоком данных с исправлением ошибок, в субблок аутентифицируемых графических данных, причем субблок аутентифицируемых графических данных дополнительно форматируют для предоставления машиночитаемого представления указанного ключа пути верификации субблока отдельно от удобочитаемого для человека представления связанного субблока

графических данных и машиночитаемого представления связанного субблока данных с исправлением ошибок; и

(iii) эталонное агрегированное хеш-значение сохраняют в реестре, или

(iv) эталонное агрегированное хеш-значение предоставляют в распоряжение пользователя,

с предоставлением тем самым на носителе для каждого субблока графических данных блока графических данных соответствующих удобочитаемых для человека графических символов вместе с соответствующими машиночитаемыми данными с исправлением ошибок, которые аутентифицируются пользователем.

8. Способ аутентификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемым представлением данных с исправлением ошибок на носителе, которые были сгенерированы согласно способу по любому из пп. 1–3, включающий этапы:

сканирования (610, 710) сканером, оснащенным блоком формирования изображения, блоком обработки сканера, имеющим память сканера и подключенным к дисплею сканера, удобочитаемых для человека графических символов на носителе для получения (620, 720) путем обработки изображения сканированных удобочитаемых для человека графических символов блока сканированных графических данных, представляющего собой цифровое представление указанных сканированных удобочитаемых для человека графических символов;

сканирования (615, 715) сканером машиночитаемого представления данных с исправлением ошибок на носителе для получения (625, 725) с помощью машиночитаемого декодера, запрограммированного в блоке обработки сканера, соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок, причем блок сканированных данных с исправлением ошибок представляет собой цифровое представление указанных сканированных данных с исправлением ошибок;

исправления (630, 730) блока сканированных графических данных с помощью кода с исправлением ошибок, запрограммированного в блоке обработки сканера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения (660, 760) визуального представления блока исправленных сканированных графических данных как соответствующих исправленных удобочитаемых для человека графических символов на дисплее сканера и сравнения отображаемого визуального представления блока исправленных сканированных графических данных с удобочитаемыми для человека графическими символами, предоставленными на носителе, для обнаружения любого изменения или мошенничества, или

(b) указания (670, 770) сканером того, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения (680, 780) данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти сканера.

9. Способ по п. 8, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 4, причем хеш-функция запрограммирована в блоке обработки сканера, и сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включающий дополнительные этапы:

вычисления по п. 4 с помощью хеш-функции, запрограммированной в блоке обработки сканера, хеш-значения сканирования блока исправленных сканированных графических данных, или блока сканированных данных с исправлением ошибок, или любой части блока данных, полученной в результате

конкатенации блока исправленных сканированных графических данных и блока сканированных данных с исправлением ошибок;

получения эталонного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное хеш-значение с хеш-значением сканирования; и

(e) указания результата операции проверки, или

(f) сохранения результата операции проверки в

памяти сканера.

10. Способ по п. 8, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 5, при этом:

операция сканирования удобочитаемых для человека графических символов на носителе включает сканирование графических символов соответствующего субблока графических данных для получения путем обработки изображения соответствующего субблока сканированных графических данных как цифрового представления сканированных графических символов субблока;

операция сканирования машиночитаемых данных с исправлением ошибок на носителе включает сканирование данных с исправлением ошибок соответствующего субблока данных с исправлением ошибок для получения соответствующего субблока сканированных данных с исправлением ошибок;

операция исправления блока сканированных графических данных включает исправление графических данных субблока сканированных графических данных с использованием соответствующего субблока сканированных данных с исправлением ошибок для получения соответствующего субблока исправленных сканированных графических данных; и

операция (a) отображения визуального представления блока исправленных сканированных данных включает отображение визуального представления субблока исправленных сканированных графических данных;

операция (b) указания того, содержит ли блок сканированных графических данных ошибку, включает указание того, содержит ли субблок сканированных графических данных ошибку;

операция (c) сохранения данных результата сканирования включает сохранение того, содержит ли субблок сканированных графических данных ошибку.

11. Способ по п. 10, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 6, причем хеш-функция и код с исправлением ошибок запрограммированы в блоке обработки сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления хеш-значения субблока на носителе блоком обработки сканера, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, включающий дополнительные этапы:

вычисления для каждой части носителя с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования соответствующего субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации указанного субблока исправленных сканированных графических данных и указанного субблока сканированных данных с исправлением ошибок;

в случае если невозможно вычислить хеш-значение субблока сканирования для части носителя, сканирования и декодирования машиночитаемого

представления хеш-значения субблока на указанной части носителя для получения соответствующего декодированного хеш-значения субблока, а также использования этого декодированного хеш-значения субблока как хеш-значения субблока сканирования для этой части носителя;

вычисления агрегированного хеш-значения сканирования как конкатенации всех хеш-значений субблока сканирования;

получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

указания результата операции проверки сканером.

12. Способ по п. 10, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на каждой части носителя были сгенерированы согласно способу по п. 7, причем эталонное агрегированное хеш-значение сохранено в реестре, сканер подключен к блоку связи сканера, выполненному с возможностью установления связи через канал связи с реестром, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включающий дополнительные этапы:

вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока

исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

получения эталонного агрегированного хеш-значения, сохраненного в реестре, блоком связи сканера и каналом связи и проверки того, совпадает ли полученное эталонное агрегированное хеш-значение с агрегированным хеш-значением сканирования; и

указания результата операции проверки сканером.

13. Способ по п. 10, отличающийся тем, что удобочитаемые для человека графические символы и машиночитаемые данные с исправлением ошибок на носителе были сгенерированы согласно способу по п. 7, причем эталонное агрегированное хеш-значение, представленное в распоряжение пользователя, сохранено в памяти сканера, и сканер дополнительно выполнен с возможностью считывания и декодирования машиночитаемого представления ключа пути верификации субблока на соответствующей части носителя и вычисления агрегированного хеш-значения из пары соответствующего хеш-значения субблока и ключа пути верификации субблока, включающий дополнительные этапы:

вычисления с помощью хеш-функции, запрограммированной в блоке обработки сканера, и согласно операциям, осуществляемым для вычисления хеш-значения субблока, хеш-значения субблока сканирования выбранного субблока

исправленных сканированных графических данных, или соответствующего субблока сканированных данных с исправлением ошибок, или любой части субблока данных, полученной в результате конкатенации субблока исправленных сканированных графических данных и субблока сканированных данных с исправлением ошибок;

сканирования сканером машиночитаемого представления ключа пути верификации субблока, что соответствует выбранному субблоку исправленных сканированных графических данных, на соответствующей части носителя и извлечения соответствующего сканированного ключа пути верификации субблока;

сканирования на носителе эталонного агрегированного хеш-значения для получения сканированного эталонного агрегированного хеш-значения;

вычисления агрегированного хеш-значения сканирования с помощью вычисленного хеш-значения субблока сканирования и сканированного ключа пути верификации субблока;

проверки того, совпадает ли эталонное агрегированное хеш-значение, сохраненное в памяти сканера, с агрегированным хеш-значением сканирования; и

указания результата операции проверки сканером.

14. Способ аутентификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее компьютера, которые были сгенерированы согласно способу по любому из пп. 1–3, причем компьютер имеет приложение для сканирования, запрограммированное в процессоре, выполненном с возможностью сканирования отображаемых удобочитаемых для человека графических символов и машиночитаемых данных с исправлением ошибок, включающий этапы:

сканирования отображаемых удобочитаемых для человека графических символов с помощью приложения для сканирования, запущенного в процессоре компьютера, для получения блока сканированных графических данных, представляющего собой цифровое представление сканированных удобочитаемых для человека графических символов;

сканирования отображаемых машиночитаемых данных с исправлением ошибок и с помощью машиночитаемого декодера приложения для сканирования, запущенного в процессоре компьютера, декодирования сканированных машиночитаемых данных с исправлением ошибок для получения соответствующих сканированных данных с исправлением ошибок в блоке сканированных данных с исправлением ошибок;

исправления блока сканированных графических данных с помощью кода с исправлением ошибок приложения для сканирования, запущенного в процессоре компьютера, с использованием сканированных данных с исправлением ошибок блока сканированных данных с исправлением ошибок для получения соответствующего блока исправленных сканированных графических данных; и

(a) отображения визуального представления блока исправленных сканированных графических данных как исправленных удобочитаемых для человека графических символов на дисплее и сравнения отображаемого визуального представления блока исправленных сканированных графических данных с удобочитаемыми для человека графическими символами, предоставленными на дисплее, для обнаружения любого изменения или мошенничества, или

(b) отображения сообщения, указывающего на то, содержит ли блок сканированных графических данных ошибку, или

(c) сохранения данных результата сканирования, указывающих на то, содержит ли блок сканированных графических данных ошибку, в памяти компьютера.

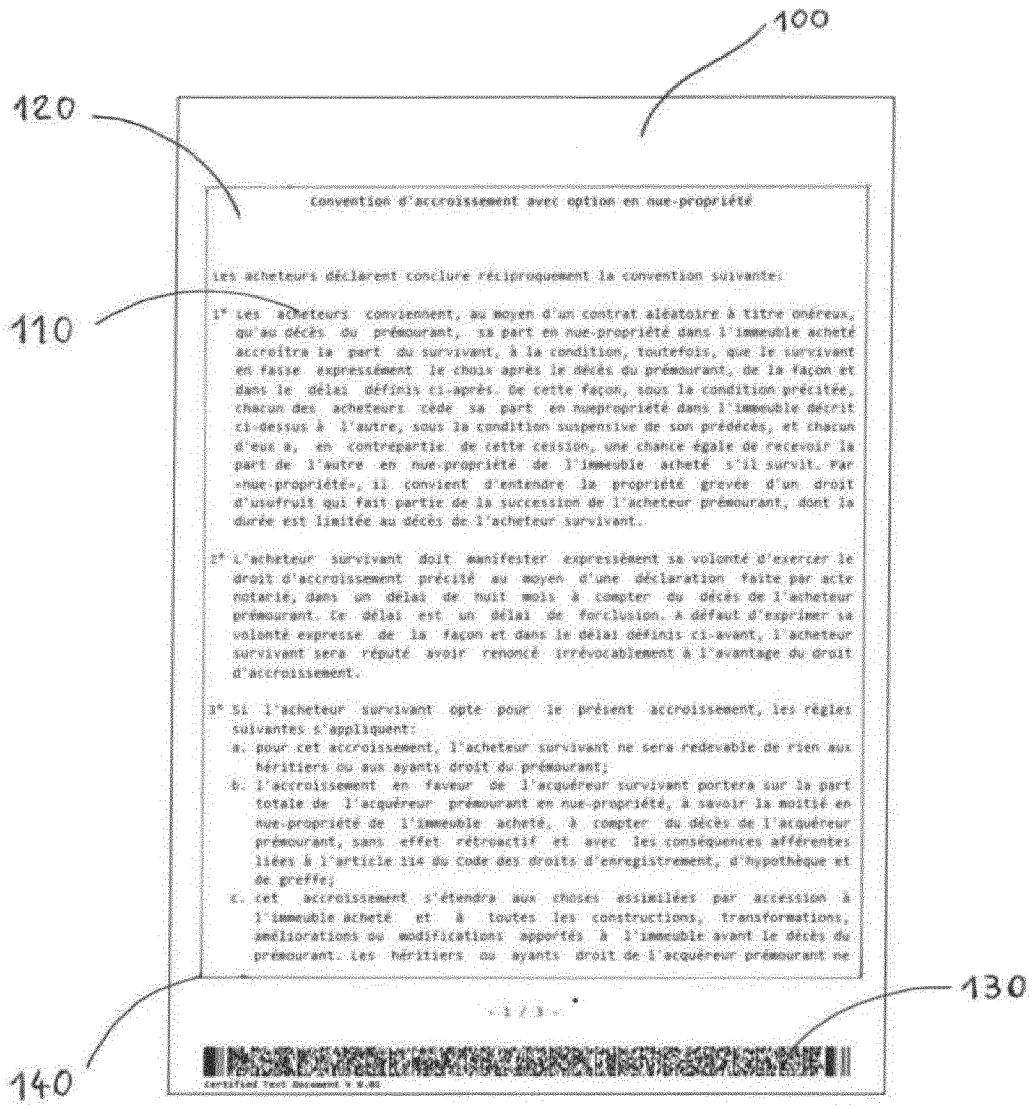
15. Носитель, маркированный данными аутентификации, содержащими удобочитаемые для человека графические символы и соответствующие

машиночитаемые данные с исправлением ошибок согласно способу по любому из пп. 1–7.

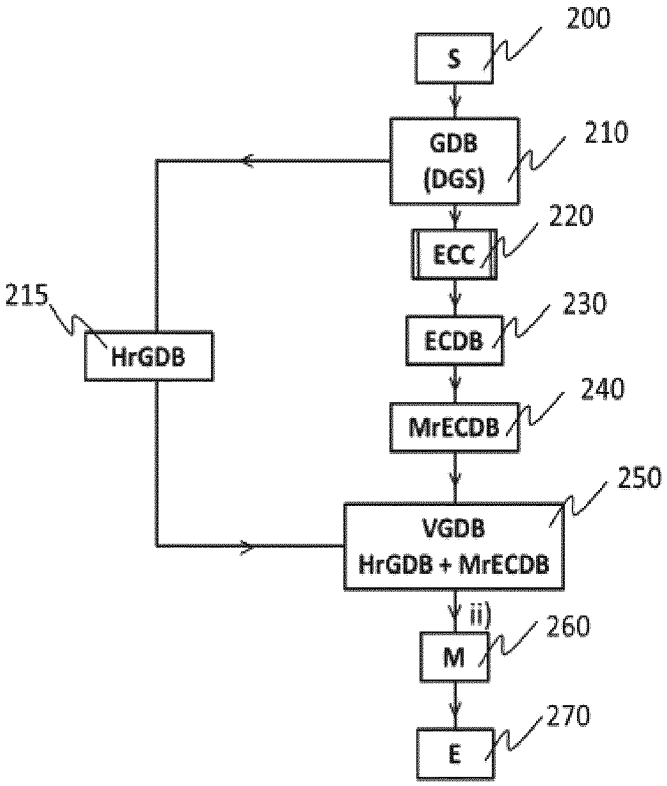
16. Сканер, оснащенный блоком формирования изображения, блоком обработки сканера и дисплеем сканера, отличающийся тем, что блок обработки сканера запрограммирован на запуск сканера, выполненного с возможностью реализации этапов способа по любому из пп. 8, 10 и 13.

17. Сканер по п. 16, дополнительно оснащенный блоком связи сканера, выполненным с возможностью установления связи через канал связи с реестром, отличающийся тем, что блок обработки сканера дополнительно запрограммирован на запуск сканера, выполненного с возможностью реализации этапов способа по любому из пп. 9, 11 и 12.

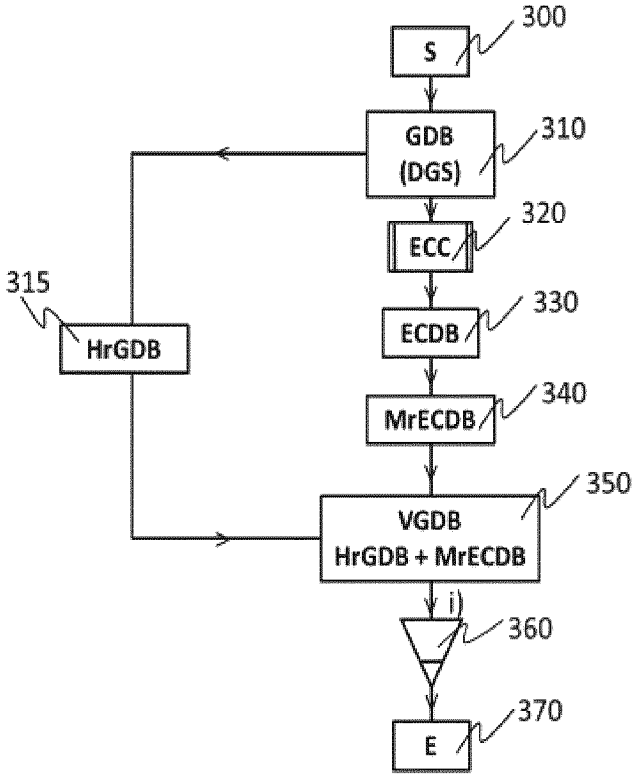
18. Компьютерный программный продукт, выполненный с возможностью, при запуске на компьютере, оснащенном процессором, памятью и дисплеем, реализации этапов способа по п. 14 для аутентификации удобочитаемых для человека графических символов, предоставленных вместе с машиночитаемыми данными с исправлением ошибок на дисплее, которые были сгенерированы согласно способу по любому из пп. 1–3.


100
120
110
130
140
Convention d'accroissement avec option en nue-propriété
les acheteurs déclarent conclure réciproquement la convention suivante:
1° les acheteurs conviennent, au moyen d'un contrat aléatoire à titre onéreux, qu'au décès du prémourant, sa part en nue-propriété dans l'immeuble acheté accroîtra la part du survivant, à la condition, toutefois, que le survivant en fasse expressément le choix après le décès du prémourant, de la façon et dans le délai définis ci-après. De cette façon, sous la condition précitée, chacun des acheteurs cède sa part en nuepropriété dans l'immeuble décrit ci-dessus à l'autre, sous la condition suspensive de son prédécès, et chacun d'eux a, en contrepartie de cette cession, une chance égale de recevoir la part de l'autre en nue-propriété de l'immeuble acheté s'il survit. Par «nue-propriété», il convient d'entendre la propriété grevée d'un droit d'usufruit qui fait partie de la succession de l'acheteur prémourant, dont la durée est limitée au décès de l'acheteur survivant.
2° L'acheteur survivant doit manifester expressément sa volonté d'exercer le droit d'accroissement précité au moyen d'une déclaration faite par acte notarié, dans un délai de huit mois à compter du décès de l'acheteur prémourant. Ce délai est un délai de forclusion. A défaut d'exprimer sa volonté expresse de la façon et dans le délai définis ci-avant, l'acheteur survivant sera réputé avoir renoncé irrévocablement à l'avantage du droit d'accroissement.
3° Si l'acheteur survivant opte pour le présent accroissement, les règles suivantes s'appliquent:
a. pour cet accroissement, l'acheteur survivant ne sera redevable de rien aux héritiers ou aux ayants droit du prémourant;
b. l'accroissement en faveur de l'acquéreur survivant portera sur la part totale de l'acquéreur prémourant en nue-propriété, à savoir la moitié en nue-propriété de l'immeuble acheté, à compter du décès de l'acquéreur prémourant, sans effet rétroactif et avec les conséquences afférentes liées à l'article 114 du Code des droits d'enregistrement, d'hypothèque et de greffe;
c. cet accroissement s'étendra aux choses assimilées par accession à l'immeuble acheté et à toutes les constructions, transformations, améliorations ou modifications apportés à l'immeuble avant le décès du prémourant. Les héritiers ou ayants droit de l'acquéreur prémourant ne
- 1 / 3 -
Certified Text Document V 0.01

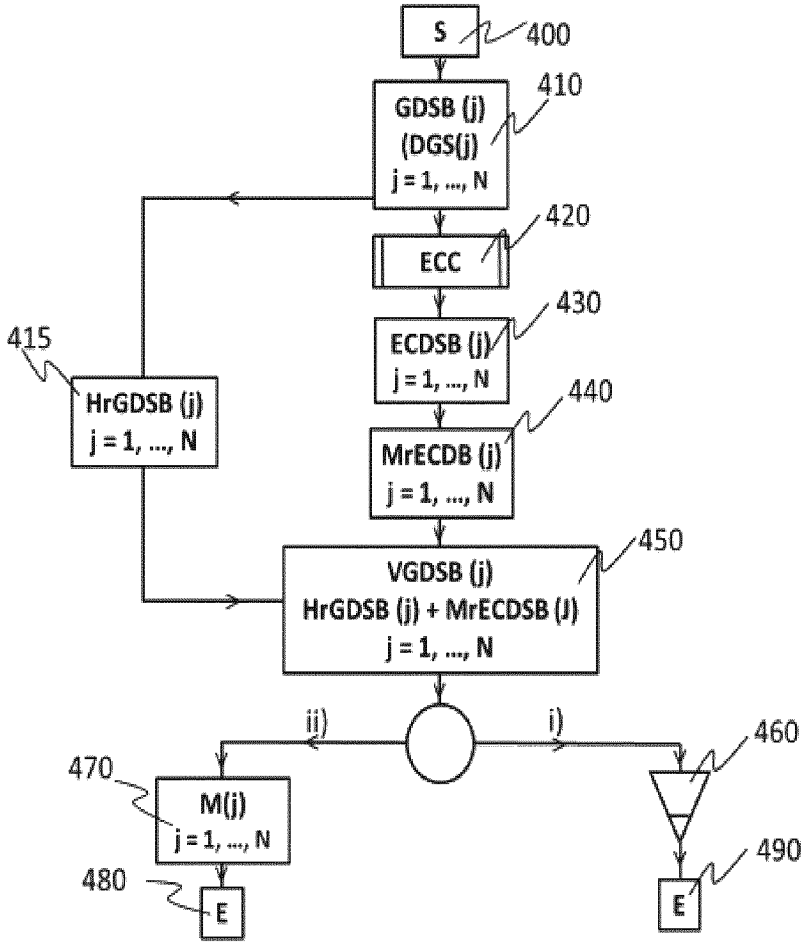
Фиг. 1


200
S
GDB
(DGS)
210
220
ECC
215
HrGDB
230
ECDB
240
MrECDB
250
VGDB
HrGDB + MrECDB
ii)
260
M
270
E

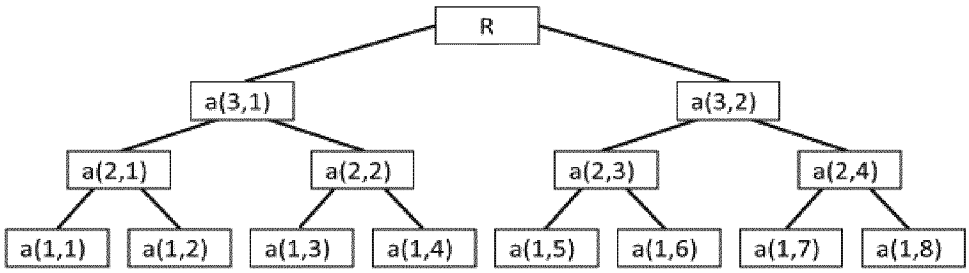
Фиг. 2


S
300
GDB
(DGS)
310
ECC
320
315
HrGDB
ECDB
330
MrECDB
340
VGDB
HrGDB + MrECDB
350
i)
360
E
370

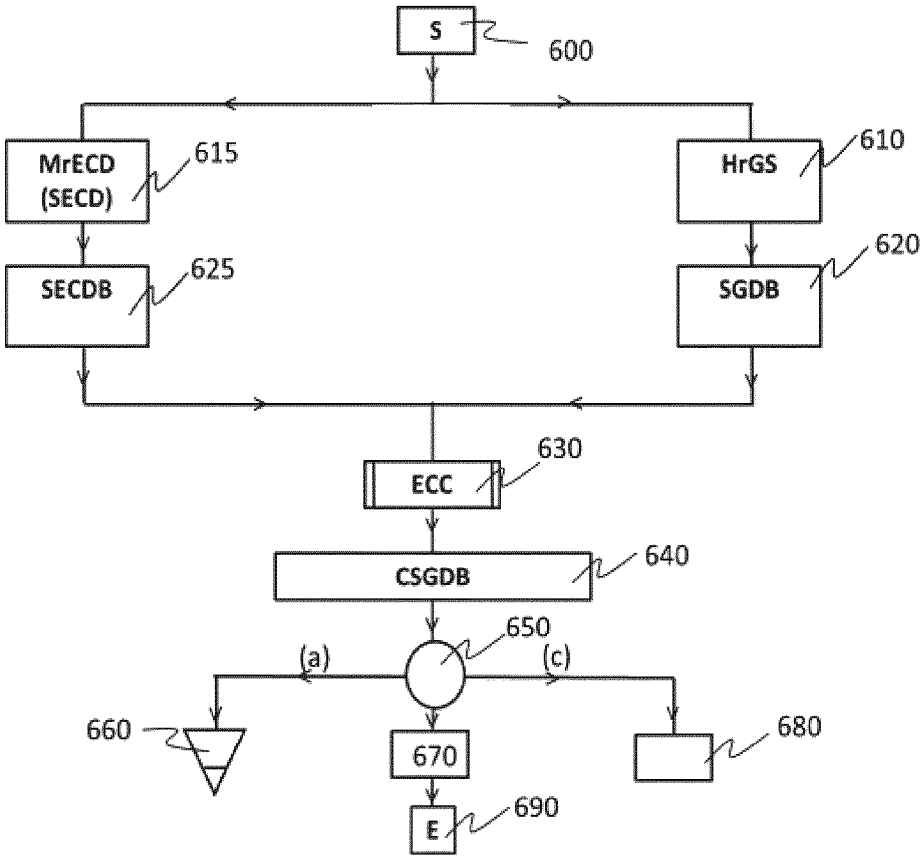
Фиг. 3


S
400
GDSB (j)
(DGS(j)
j = 1, ..., N
410
ECC
420
ECDSB (j)
j = 1, ..., N
430
415
HrGDSB (j)
j = 1, ..., N
MrECDB (j)
j = 1, ..., N
440
VGDSB (j)
HrGDSB (j) + MrECDSB (J)
j = 1, ..., N
450
ii)
i)
460
470
M(j)
j = 1, ..., N
480
E
490
E

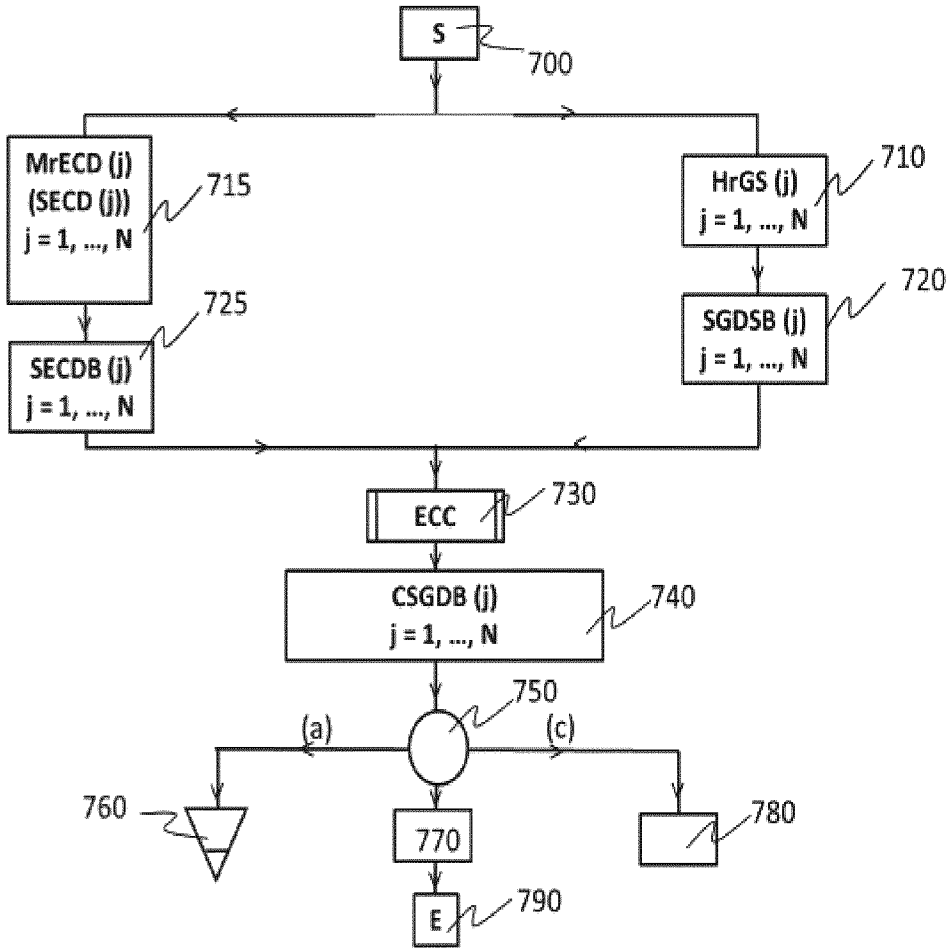
Фиг. 4



Фиг. 5


S
600
MrECD
(SECD)
615
HrGS
610
SECDB
625
SGDB
620
ECC
630
CSGDB
640
650
(a)
(c)
660
670
680
E
690

Фиг. 6


S
700
MrECD (j)
(SECD (j))
j = 1, ..., N
715
HrGS (j)
j = 1, ..., N
710
SECDB (j)
j = 1, ..., N
725
SGDSB (j)
j = 1, ..., N
720
ECC
730
CSGDB (j)
j = 1, ..., N
740
750
(a)
(c)
760
770
780
E
790

Фиг. 7