(19) Евразийское патентное ведомство

(21) 202191516 (13) A1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОЙ ЗАЯВКЕ

(43) Дата публикации заявки
2022.09.30

(22) Дата подачи заявки
2021.06.29

(51) Int. Cl. ***G06F 21/16*** (2006.01)
G06T 1/00 (2006.01)

(54) СПОСОБ И СИСТЕМА ЗАЩИТЫ ЦИФРОВОЙ ИНФОРМАЦИИ, ОТОБРАЖАЕМОЙ НА ЭКРАНЕ ЭЛЕКТРОННЫХ УСТРОЙСТВ, С ПОМОЩЬЮ ДИНАМИЧЕСКИХ ЦИФРОВЫХ МЕТОК

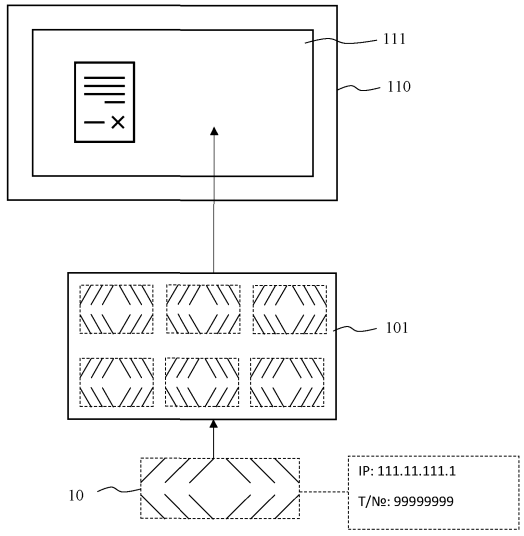
(31) **2021107967**
(32) **2021.03.25**
(33) **RU**

(71) Заявитель:
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО "СБЕРБАНК РОССИИ" (ПАО СБЕРБАНК) (RU)

(72) Изобретатель:
Оболенский Иван Александрович, Кузьмин Александр Михайлович, Сысоев Валентин Валерьевич, Ястрембский Андрей Николаевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение относится к области защиты цифровых данных, в частности конфиденциальной и чувствительной информации, отображаемой на экране (111) электронного устройства (110), с помощью внедрения цифровых меток (ЦМ) (10). Технический результат заключается в повышении устойчивости защиты информации за счет изменения яркостной характеристики на заданную величину сформированного защитного слоя на основе цифровых меток. Заявленный результат достигается за счет осуществления компьютерно-реализуемого способа защиты данных, отображаемых на экране (111) вычислительных устройств (ВУ) (110), выполняемого с помощью процессора и содержащего этапы, на которых формируют ЦМ (10) в виде блока данных, содержащего закодированную информацию, по меньшей мере идентифицирующую пользователя ВУ (110), причем закодированная информация представлена в виде динамических графических элементов, осуществляющих сканирование области их размещения на экране (111) ВУ (110); формируют невидимый защитный слой (101), состоящий из набора упомянутых блоков данных, покрывающий большую часть области отображения экрана (111) ВУ (110), и выполняют наложение защитного слоя (101) на область отображения экрана (111) ВУ (110).



202191516 A1

202191516 A1

МПК: G06F21/16

СПОСОБ И СИСТЕМА ЗАЩИТЫ ЦИФРОВОЙ ИНФОРМАЦИИ, ОТОБРАЖАЕМОЙ НА ЭКРАНЕ ЭЛЕКТРОННЫХ УСТРОЙСТВ, С ПОМОЩЬЮ ДИНАМИЧЕСКИХ ЦИФРОВЫХ МЕТОК

ОБЛАСТЬ ТЕХНИКИ

[0001] Заявленное техническое решение относится к области защиты цифровых данных, в частности конфиденциальной и чувствительной информации, отображаемой на экране электронного устройства, с помощью внедрения цифровых меток (ЦМ).

УРОВЕНЬ ТЕХНИКИ

[0002] Использование ЦМ в области защиты цифровой информации является распространенным решением, при котором в изображение внедряется закодированная информация, позволяющая идентифицировать ее принадлежность или лицо, ответственное за ее утечку и/или несанкционированный доступ.

[0003] Как правило такие подходы используют заданный графический элемент или область изображения, содержащую ЦМ. При этом такая метка может быть как различимой, так и неразличимой для человеческого глаза. Одним из примеров неразличимой метки является стеганография.

[0004] Аналогом предлагаемого решения является принцип формирования на основании ЦМ защитного слоя, раскрытого в патенте США 9,239,910 (Markany Inc, 19.01.2016). Решение заключается в создании невидимого защитного слоя, состоящего из цифровых меток, который используется как фоновый слой, отображаемой на экране устройства и невидимый для пользователя.

[0005] Недостатком существующего подхода является его недостаточная эффективность, обусловленная тем, что для формирования защитного слоя используется ЦМ, представляющая собой текст или графический примитив, выбираемый из базы данных и применяемый для последующего генерирования заполнения пространства. Это приводит к тому, что такое формирование слоя становится чувствительным к качеству и при последующем захвате изображения на экране с помощью внешнего устройства, например, камерой смартфона или фотоаппарата, при смене ракурса или захвате части экрана с защитным слоем, впоследствии изъятие ЦМ и установление факта утечки данных становиться достаточно сложным или невозможным.

СУЩНОСТЬ ИЗОБРЕТЕНИЯ

[0006] Предлагаемый подход позволяет решить техническую проблему, заключающуюся в низкой устойчивости (робастности) метода защиты цифровых данных при их фиксации внешними средствами с различных ракурсов и качеством съемки, что приводит к снижению эффективности такого принципа защиты цифровых данных.

[0007] Технический результат заключается в повышении эффективности способа защиты цифровых данных на экранах устройств, за счет повышения устойчивости цифровых меток при их динамическом сканировании области размещения на экране с формированием невидимого защитного слоя.

[0008] Заявленный результат достигается за счет осуществления компьютерно-реализуемого способа компьютерно-реализуемого способа защиты данных, отображаемых на экране вычислительного устройства (ВУ), выполняемого процессором и содержащего этапы, на которых:

формируют цифровую метку (ЦМ) в виде блока данных, содержащего закодированную информацию, по меньшей мере идентифицирующую пользователя ВУ, причем закодированная информация представлена в виде динамических графических элементов, осуществляющих сканирование области их размещения на экране ВУ;

формируют невидимый защитный слой, состоящий из набора упомянутых блоков данных, покрывающий большую часть области отображения экрана ВУ, и

выполняют наложение защитного слоя на область отображения экрана ВУ.

[0009] В одном частных примеров реализации способа в ЦМ кодируется дополнительно информация о дате и времени.

[0010] В другом частном примере реализации способа при сканировании динамическими графическими элементами осуществляется анализ цвета пикселей в области их размещения.

[0011] В другом частном примере реализации способа на основании цвета пикселя выполняется корректировка яркости графического элемента.

[0012] В другом частном примере реализации способа корректировка осуществляется на основании параметров каждого пикселя в области размещения графического элемента в цветовой схеме RGB.

[0013] В другом частном примере реализации способа выполняется перевод цветовой схемы RGB в HSV с вычислением параметров тона H, насыщенности S, и яркости V.

[0014] В другом частном примере реализации способа полученный параметр яркости V изменяется на величину Δ.

[0015] В другом частном примере реализации способа полученный параметр яркости V_Δ вместе с параметрами H и S конвертируются в цветовую схему RGB.

[0016] В другом частном примере реализации способа динамика отображения графических элементов выбирается исходя из частоты обновления экрана ВУ.

[0017] Заявленный технический результат достигается также за счет компьютерно-реализуемого способа обработки защищенных данных, который выполняется с помощью процессора и содержит этапы, на которых:

получают изображение, содержащее по меньшей мере часть изображения экрана с информацией, защищенной с помощью способа по любому из пп.1-9;

осуществляют декодирование информации на основании ЦМ из полученного изображения, при котором:

выполняют попиксельное разложение изображения на пороговые изображения;

выполняют выявление графических элементов, формирующих ЦМ;

восстанавливают информацию из ЦМ на основании битовой последовательности, сформированной графическими элементами.

[0018] В одном из частных примеров реализации способа каждое пороговое изображение формируется как усредненный спектр RGB-палитры соответствующего порога P, на основании которого создается M – Δp изображений, на которых каждый пиксель изображения удовлетворяет условию $P \in \mathbb{N}$: {P – Δp, …, P + Δp}, где P - текущий порог, $\Delta p \in \mathbb{N}$ – дельта детекции порога.

[0019] В другом частном примере реализации способа при формировании пороговых изображений каждый пиксель переводится в формат HSV, после чего извлекается показатель насыщенности S, на основании которого создается N - Δs изображений, на которых каждый пиксель изображения удовлетворяет условию $S \in \mathbb{R}$: {S – Δs, …, S + Δs}, где S - насыщенность пикселя, $\Delta s \in \mathbb{R}$ – дельта детекции насыщения.

[0020] В другом частном примере реализации способа при формировании пороговых изображений из обрабатываемого изображения извлекаются пиксели, каждый пиксель переводится в формат HSV, выполняется извлечение показателя яркости V, на основании которого создается N - Δv изображений, на которых каждый пиксель изображения удовлетворяет условию $V \in \mathbb{R}$: {V – Δv, …, V + Δv}, где V - яркость пикселя, $\Delta v \in \mathbb{R}$ – дельта детекции яркости.

[0021] Заявленное решение также осуществляется с помощью системы для защиты данных, отображаемых на экране вычислительного устройства, которая содержит по

меньшей мере один процессор и по меньшей мере одну память, содержащую машиночитаемые инструкции, которые при их исполнении процессором осуществляют вышеуказанные способы.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0022] Фиг. 1 иллюстрирует общий принцип заявленного решения.

[0023] Фиг. 2 иллюстрирует блок-схему заявленного способа защиты данных.

[0024] Фиг. 3А иллюстрирует пример блока данных защитного слоя.

[0025] Фиг. 3Б иллюстрирует пример размещения слоя на экране устройства.

[0026] Фиг. 4 иллюстрирует блок-схему способа декодирования информации из изображения, защищенного ЦМ.

[0027] Фиг. 5 иллюстрирует пример захвата изображения информации с экрана устройства.

[0028] Фиг. 6 иллюстрирует принцип декодирования ЦМ из изображения.

[0029] Фиг. 7 иллюстрирует общий вид вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0030] На Фиг. 1 представлена общая концепция технической реализации заявленного решения. Защита чувствительной и/или конфиденциальной информации, отображаемой на экране (111) вычислительного устройства (ВУ) (110) пользователя, например, компьютера, ноутбука, планшета и т.п. Защита данных на экране (111) осуществляется с помощью внедрения ЦМ (10), в которую кодируется соответствующая информация для последующего установления места и ответственного лица, допустившего утечку или несанкционированное получение информации вне защищенного периметра инфраструктуры, например, с помощью фотографирования, видеосъемки или захвата (скриншот) изображения на экране с применением внешних устройств (смартфон, фотоаппарат и т.п.), в том числе с последующей распечаткой снимков с полученной информацией. Каждая ЦМ (10) представляет собой блок данных, формирующих невидимый защитный слой (101), который покрывает большую часть или всю область отображения на экране (111) ВУ (110).

[0031] Как представлено на Фиг. 2 заявленный способ (200) защиты цифровой информации содержит ряд последовательных этапов. На первом этапе (201) осуществляется формирование ЦМ (10). В ЦМ (10) с помощью алгоритмов двоичного (бинарного) кодирования данных может внедряться любой тип информации, например,

текстовый, графический или их сочетания. ЦМ (10) формируется из совокупности графических элементов (11, 12), которые кодируют информацию. Количество элементов (11, 12) в каждой ЦМ (10) может варьироваться исходя из объема данных, подлежащих кодированию, например, кодирование 32 бит информации требует формирование блока ЦМ (10) размера 4*8. На представленном примере ЦМ (10) элементы (11, 12) представлены в виде косых линий, однако их форма и принцип размещения может быть иным, обеспечивая соблюдения принципа разграничения кодирования информации в виде логических 0 и 1.

[0032] Как правило, данные, внедренные в ЦМ (10), необходимы для идентификации ВУ (110) или непосредственно пользователя данного устройства, например, сотрудника, имеющего доступ к чувствительной информации. Такими данными могут выступать: табельный номер, имя, фотография пользователя, IP-адрес, MAC-адрес, уникальный идентификатор ВУ. Данная информация может использоваться как по отдельности, так и в любом сочетании. Дополнительно может также кодироваться информация о времени и/или дате, например, времени формирования ЦМ (10), текущая дата. Информация о дате и времени может динамически изменяться для включения актуальной информации во время кодирования ЦМ (10).

[0033] ЦМ (10) представляет собой элемент графического интерфейса заданной битовой размерности, при этом графические элементы (11, 12), формирующие ЦМ (10), являются динамическими и осуществляют постоянное или периодическое сканирование пространства их размещения. Сканирование пространства осуществляется исходя из показателей частоты обновления экрана (111). Один элемент (11) ЦМ представляет собой логический 0, второй (12) – логическую 1. Различный принцип ориентирования элементов (11, 12) позволяет разграничить их в пространстве и сформировать паттерн блока ЦМ (10) для кодирования информации внутри нее.

[0034] На этапе (202) формируют защитный слой (101) в виде размещения ЦМ (10), которые заполняют большую часть или все пространство экрана (111). Количество ЦМ (10) определяется исходя из разрешающей способности экрана (111) и размерности ЦМ (10). Как правило, ЦМ (10) выбираются равной размерности, но могут также иметь чередующийся порядок их размещения для формирования слоя (101), что также не нарушает техническое воплощение заявленного решения в части последующей идентификации данных в процессе декодирования.

[0035] Защитный слой (101) формируется невидимым (прозрачным), чтобы не быть различимым человеческим глазом и скрыть факт применения защиты данных на экране (111).

[0036] Прозрачность слоя (101) создаваемого узора из ЦМ (10) может формироваться различными способами настройки графических изображений, например, с помощью регулировки непрозрачности изображения (opacity), с помощью Alpha-канала в RGBA палитре, с помощью Alpha-канала в HSLA палитре.

[0037] Также, в другом частном аспекте, прозрачность слоя (101) создаваемого узора из ЦМ (10) формируется изменением яркостной характеристики (на определенный параметр – дельту яркости) пикселей, на которых будет нанесена метка.

[0038] Подбор параметров для формирования невидимого слоя (101) выполняется для преодоления порога различения (https://en.wikipedia.org/wiki/Just-noticeable_difference), обеспечивая его невидимость для обычного пользователя.

[0039] После формирования защитного слоя (101) на этапе (203) выполняется его наложение на область отображения экрана (111) ВУ (110), таким образом, что вся зона охвата экрана покрывается наложенным слоем (101). Применение такого подхода позволяет определить значение ЦМ (10) в любом участке экрана (111) вне зависимости от координаты или масштаба скриншота, или фотокопии.

[0040] На Фиг. 3А – 3Б представлен пример сформированного защитного слоя (101) на основе множества ЦМ (10). Представленный пример ЦМ (10) может создаваться с применением кодирования информации в контрастных каналах цветовой схемы, например, RGB, HSL, ARGB и т.п.

[0041] Каждый элемент (11, 12) УМ (10) является динамическим и осуществляет сканирование пространства, расположенного за ним, для того чтобы попиксельно подготавливать видимость графических элементов (11, 12), обеспечивая выделение их яркости на заданную дельту. Для этого в изображении на экране (111) берется пиксель P, для которого вычисляются его параметры P(R,G,B). Далее параметры переводятся в параметры P(H,S,V), после чего из P извлекается параметр V. Далее параметр V пикселя P изменяется на дельту d, V* = V +/- d, например, d увеличивается, если V <0.5 и уменьшается, если V иное. Причем, если пиксели за графическими элементами (11, 12) ЦМ (10) имеют темный оттенок, программная логика алгоритма формирования ЦМ (10) увеличивает яркость, если светлый – уменьшает. Далее параметры пикселя P(H,S,V*) переводятся в P(R,G,B) в изображении. Благодаря этому, котором каждый пиксель метки имеет дельту яркости, незаметную для человеческого глаза, но распознаваемую, впоследствии, декодером. Это позволяет регулировать устойчивость формируемого защитного слоя (101) из меток и в то же время делать его неразличимым для пользователя.

[0042] Далее рассмотрим процесс декодирования информации, защищенной ЦМ, представленной на Фиг. 4 – Фиг. 6.

[0043] Фиг. 4 иллюстрирует блок-схему выполнения способа (300) декодирования информации из захватываемого изображения. На первом этапе (301) на вычислительный модуль (например, процессор) поступает изображение (410), которое было сделано с помощью внешнего устройства (400) и содержит часть или полностью информацию, представленную на экране (111) ВУ (110), как это представлено на Фиг. 5.

[0044] Далее полученное изображение (410) проходит этап обработки (302). На первой стадии выполнения этапа (302) осуществляется попиксельное разложение изображения на пороговые изображения (этап 3021) или пороги. Порог – это среднее арифметическое значений RGB каналов изображения. Поскольку ЦМ (10) представляет собой однородный объект, имеющий одинаковую дельту, что вызывает ее проявление на изображении при определенном значении порога в произвольной области декодируемого изображения (410), что позволяет хорошо отображать артефакты на фотографии, вызванные из-за фотографирования экрана (111), обладающего определенной частотой обновления, не совпадающей с временем открытия диафрагмы устройства (400), с помощью которого выполняется фото- или видеосъемка. В данном случае сама ЦМ (10) является артефактом.

[0045] Каждое пороговое изображение формируется как усредненный спектр RGB-палитры соответствующего порога P, на основании которого создается M – Δp изображений, на которых каждый пиксель изображения удовлетворяет условию $P \in \mathbb{N}$: $\{P - \Delta p, \ldots, P + \Delta p\}$, где P - текущий порог, $\Delta p \in \mathbb{N}$ – дельта детекции порога.

[0046] Также, в другом частном аспекте, формировании пороговых изображений может выполняться способом, при котором каждый пиксель переводится в формат HSV, после чего извлекается показатель насыщенности S, на основании которого создается N - Δs изображений, на которых каждый пиксель изображения удовлетворяет условию $S \in \mathbb{R}$: $\{S - \Delta s, \ldots, S + \Delta s\}$, где S - насыщенность пикселя, $\Delta s \in \mathbb{R}$ – дельта детекции насыщения.

[0047] Еще одним способом при формировании пороговых изображений из обрабатываемого изображения извлекаются пиксели, каждый пиксель переводится в формат HSV, выполняется извлечение показателя яркости V, на основании которого создается N - Δv изображений, на которых каждый пиксель изображения удовлетворяет условию $V \in \mathbb{R}$: $\{V - \Delta v, \ldots, V + \Delta v\}$, где V - яркость пикселя, $\Delta v \in \mathbb{R}$ – дельта детекции яркости.

[0048] На следующем этапе (3022) декодирования выявляются графические элементы (11, 12), формирующие одну или несколько ЦМ (10), которые попали в изображение (410). При обработке определяется местоположение элементов (11, 12) для последующего накопления и формирования их последовательности для этапа (3023), на котором

осуществляется восстановление информацию из ЦМ на основании битовой последовательности, сформированной выявленными графическими элементами (11, 12).

[0049] Создание предобработанного изображения осуществляется следующим образом. На каждом пороге отмечаются местоположения распознанных элементов (11) и (12), они сохраняются в памяти устройства (ОЗУ), при этом обозначения как для элементов (11), так и для (12) разные, к примеру, для (11) – красная геометрическая фигура (квадрат), для (12) – зеленая. На новом полотне (изображении) размещаются из памяти все найденные выше элементы (11,12), причем размещение происходит, соблюдая цветовую гамму, описанную выше. В случае коллизии осуществляется выбор той геометрической фигуры, которая на данное место попало наибольшее число раз.

[0050] Как представлено на Фиг. 6 в результате декодирования предобработанного изображения (410) определяются ЦМ (10) на защитном слое (101) и извлекается информация из элементов (11, 12), закодированная в битовую последовательность ЦМ (10), по которой устанавливается принадлежность ВУ (110) конкретному сотруднику, а также любая иная дополнительная информация, закодированная в ЦМ (10).

[0051] На Фиг. 7 представлен общий вид вычислительного устройства (500), пригодного для выполнения способов (200, 300). Устройство (500) может представлять собой, например, сервер или иной тип вычислительного устройства, который может применяться для реализации заявленного технического решения. В том числе входить в состав облачной вычислительной платформы.

[0052] В общем случае вычислительное устройство (500) содержит объединенные общей шиной информационного обмена один или несколько процессоров (501), средства памяти, такие как ОЗУ (502) и ПЗУ (503), интерфейсы ввода/вывода (504), устройства ввода/вывода (505), и устройство для сетевого взаимодействия (506).

[0053] Процессор (501) (или несколько процессоров, многоядерный процессор) могут выбираться из ассортимента устройств, широко применяемых в текущее время, например, компаний Intel™, AMD™, Apple™, Samsung Exynos™, MediaTEK™, Qualcomm Snapdragon™ и т.п. В качестве процессора (501) может также применяться графический процессор, например, Nvidia, AMD, Graphcore и пр.

[0054] ОЗУ (502) представляет собой оперативную память и предназначено для хранения исполняемых процессором (501) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (502), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

[0055] ПЗУ (503) представляет собой одно или более устройств постоянного хранения данных, например, жесткий диск (HDD), твердотельный накопитель данных (SSD), флэш-память (EEPROM, NAND и т.п.), оптические носители информации (CD-R/RW, DVD-R/RW, BlueRay Disc, MD) и др.

[0056] Для организации работы компонентов устройства (500) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов B/B (504). Выбор соответствующих интерфейсов зависит от конкретного исполнения вычислительного устройства, которые могут представлять собой, не ограничиваясь: PCI, AGP, PS/2, IrDa, FireWire, LPT, COM, SATA, IDE, Lightning, USB (2.0, 3.0, 3.1, micro, mini, type C), TRS/Audio jack (2.5, 3.5, 6.35), HDMI, DVI, VGA, Display Port, RJ45, RS232 и т.п.

[0057] Для обеспечения взаимодействия пользователя с вычислительным устройством (500) применяются различные средства (505) B/B информации, например, клавиатура, дисплей (монитор), сенсорный дисплей, тач-пад, джойстик, манипулятор мышь, световое перо, стилус, сенсорная панель, трекбол, динамики, микрофон, средства дополненной реальности, оптические сенсоры, планшет, световые индикаторы, проектор, камера, средства биометрической идентификации (сканер сетчатки глаза, сканер отпечатков пальцев, модуль распознавания голоса) и т.п.

[0058] Средство сетевого взаимодействия (506) обеспечивает передачу данных устройством (500) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (506) может использоваться, но не ограничиваться: Ethernet карта, GSM модем, GPRS модем, LTE модем, 5G модем, модуль спутниковой связи, NFC модуль, Bluetooth и/или BLE модуль, Wi-Fi модуль и др.

[0059] Дополнительно могут применяться также средства спутниковой навигации в составе устройства (500), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0060] Представленные материалы заявки раскрывают предпочтительные примеры реализации технического решения и не должны трактоваться как ограничивающие иные, частные примеры его воплощения, не выходящие за пределы испрашиваемой правовой охраны, которые являются очевидными для специалистов соответствующей области техники.

ФОРМУЛА

1. Компьютерно-реализуемый способ защиты данных, отображаемых на экране вычислительного устройства (ВУ), выполняемый процессором и содержащий этапы, на которых:

- формируют цифровую метку (ЦМ) в виде блока данных, содержащего закодированную информацию, по меньшей мере идентифицирующую пользователя ВУ, причем закодированная информация представлена в виде динамических графических элементов, осуществляющих сканирование области их размещения на экране ВУ;
- формируют невидимый защитный слой, состоящий из набора упомянутых блоков данных, покрывающий большую часть области отображения экрана ВУ, и
- выполняют наложение защитного слоя на область отображения экрана ВУ.

2. Способ по п.1, характеризующийся тем, что в ЦМ кодируется дополнительно информация о дате и времени.

3. Способ по п.1, характеризующийся тем, что при сканировании динамическими графическими элементами осуществляется анализ цвета пикселей в области их размещения.

4. Способ по п.3, характеризующийся тем, что на основании цвета пикселя выполняется корректировка яркости графического элемента.

5. Способ по п.4, характеризующийся тем, что корректировка осуществляется на основании параметров каждого пикселя в области размещения графического элемента в цветовой схеме RGB.

6. Способ по п.5, характеризующийся тем, что выполняется перевод цветовой схемы RGB в HSV с вычислением параметров тона H, насыщенности S, и яркости V.

7. Способ по п.6 характеризующийся тем, что полученный параметр яркости V изменяется на величину Δ.

8. Способ по п.7 характеризующийся тем, что полученный параметр яркости V_{Δ} вместе с параметрами H и S конвертируются в цветовую схему RGB.

9. Способ по п.1, характеризующийся тем, что динамика отображения графических элементов выбирается исходя из частоты обновления экрана ВУ.

10. Компьютерно-реализуемый способ обработки защищенных данных, выполняемый с помощью процессора и содержащий этапы, на которых:

- получают изображение, содержащее по меньшей мере часть изображения экрана с информацией, защищенной с помощью способа по любому из пп.1-9;

– осуществляют декодирование информации на основании ЦМ из полученного изображения, при котором:

выполняют попиксельное разложение изображения на пороговые изображения;

выполняют выявление графических элементов, формирующих ЦМ;

восстанавливают информацию из ЦМ на основании битовой последовательности, сформированной графическими элементами.

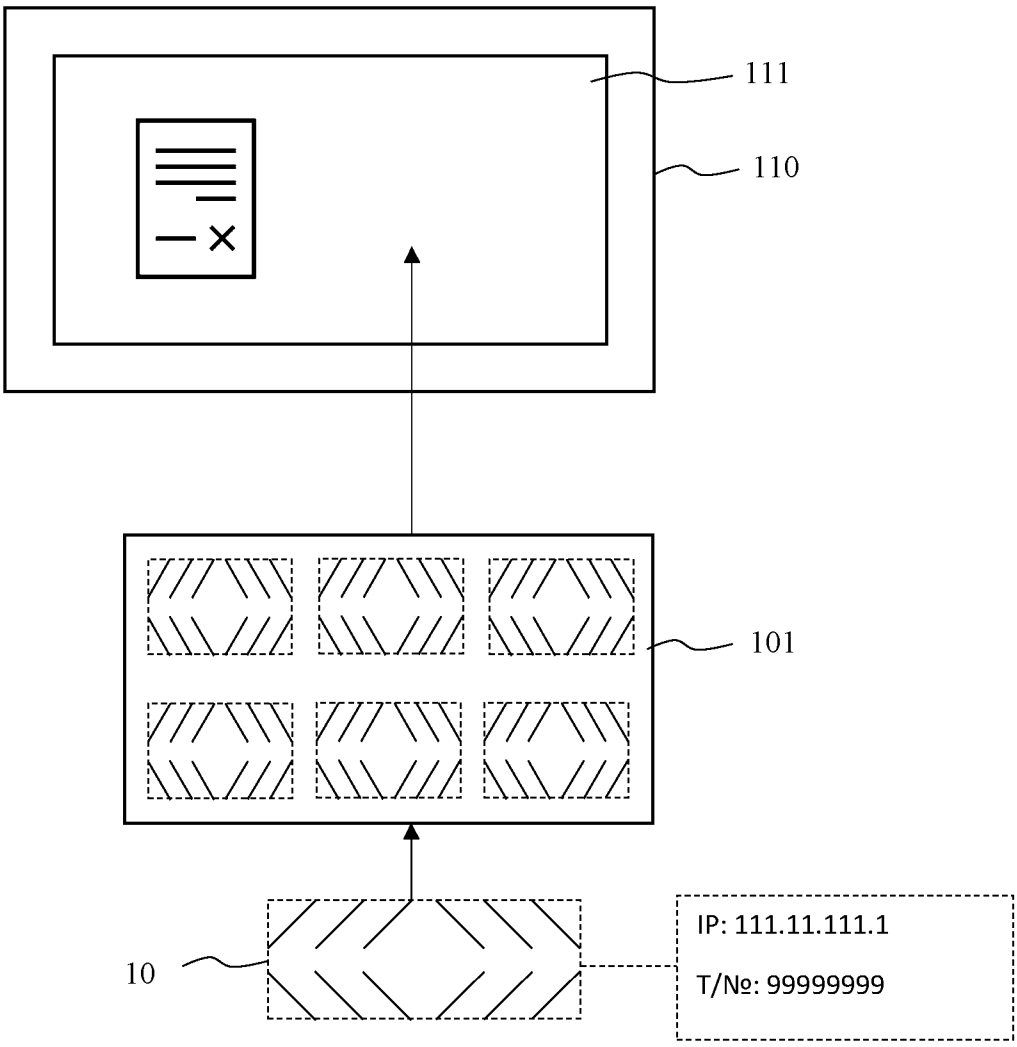
11. Способ по п.10, характеризующийся тем, что каждое пороговое изображение формируется как усредненный спектр RGB-палитры соответствующего порога P, на основании которого создается M – Δp изображений, на которых каждый пиксель изображения удовлетворяет условию $P \in \mathbb{N}$: {P – Δp, …, P + Δp}, где P - текущий порог, $\Delta p \in \mathbb{N}$ – дельта детекции порога.

12. Способ по п.10, характеризующийся тем, что при формировании пороговых изображений каждый пиксель переводится в формат HSV, после чего извлекается показатель насыщенности S, на основании которого создается N - Δs изображений, на которых каждый пиксель изображения удовлетворяет условию $S \in \mathbb{R}$: {S – Δs, …, S + Δs}, где S - насыщенность пикселя, $\Delta s \in \mathbb{R}$ – дельта детекции насыщения.

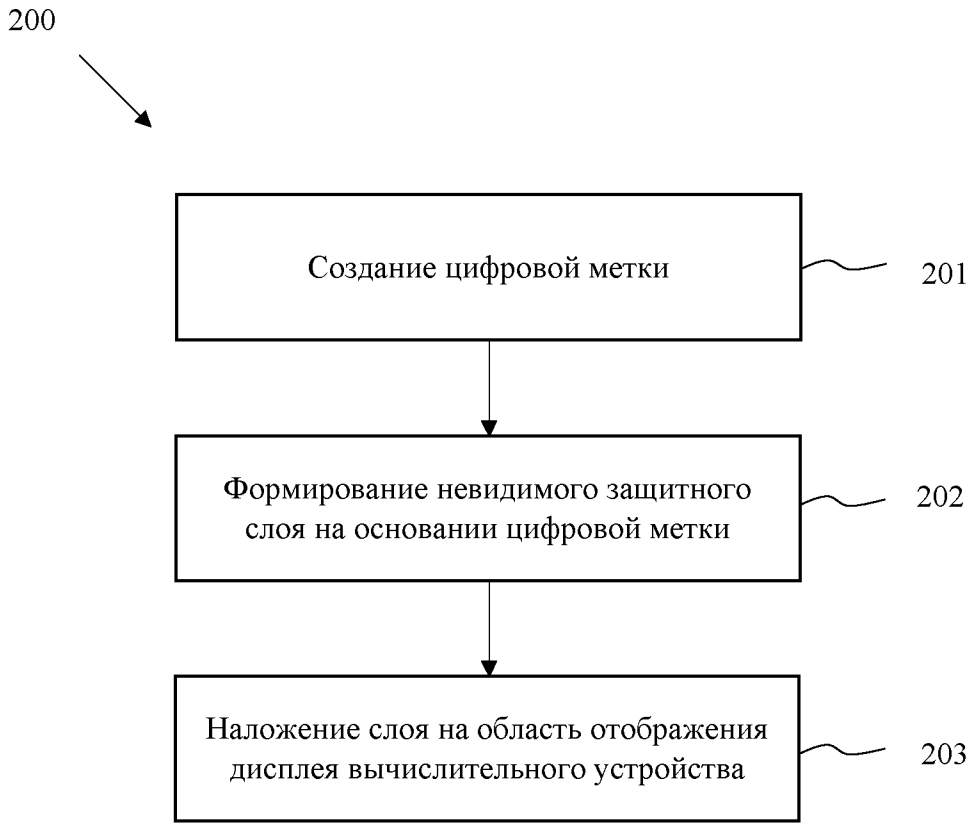
13. Способ по п.10, характеризующийся тем, что при формировании пороговых изображений из обрабатываемого изображения извлекаются пиксели, каждый пиксель переводится в формат HSV, выполняется извлечение показателя яркости V, на основании которого создается N - Δv изображений, на которых каждый пиксель изображения удовлетворяет условию $V \in \mathbb{R}$: {V – Δv, …, V + Δv}, где V - яркость пикселя, $\Delta v \in \mathbb{R}$ – дельта детекции яркости.

14. Система для защиты данных, отображаемых на экране вычислительного устройства, содержащая по меньшей мере один процессор и по меньшей мере одну память, содержащую машиночитаемые инструкции, которые при их исполнении процессором осуществляют способ по любому из пп. 1-9.

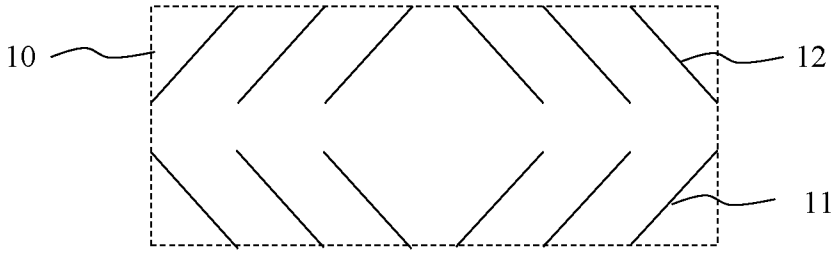
15. Система для обработки защищенных данных, содержащая по меньшей мере один процессор и по меньшей мере одну память, содержащую машиночитаемые инструкции, которые при их исполнении процессором осуществляют способ по любому из пп. 10-13.



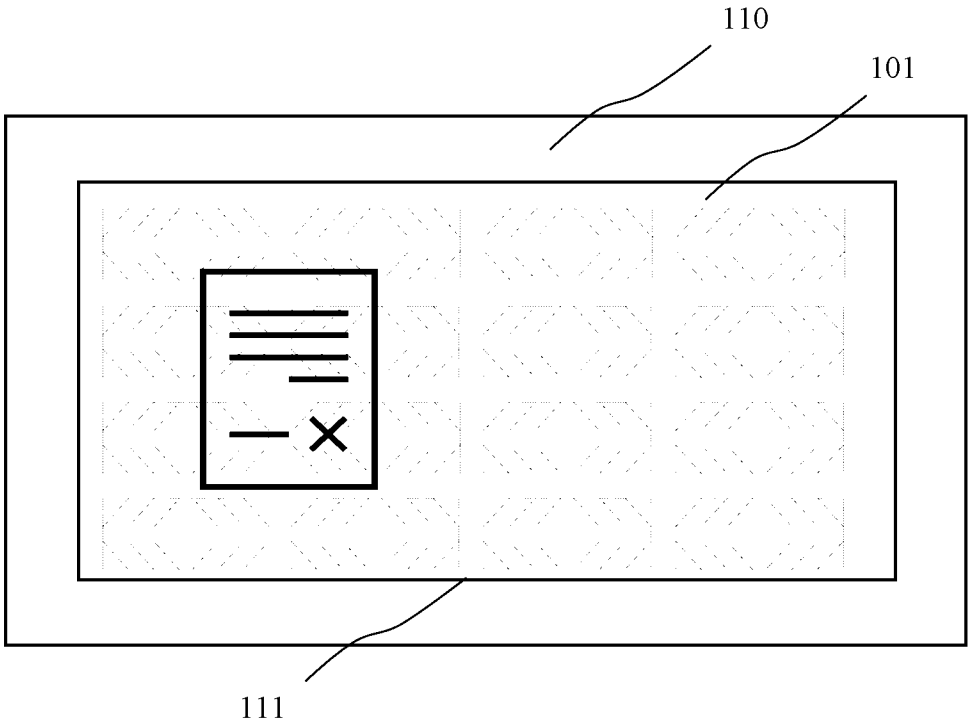
Фиг. 1


200
Создание цифровой метки
201
Формирование невидимого защитного слоя на основании цифровой метки
202
Наложение слоя на область отображения дисплея вычислительного устройства
203

Фиг. 2



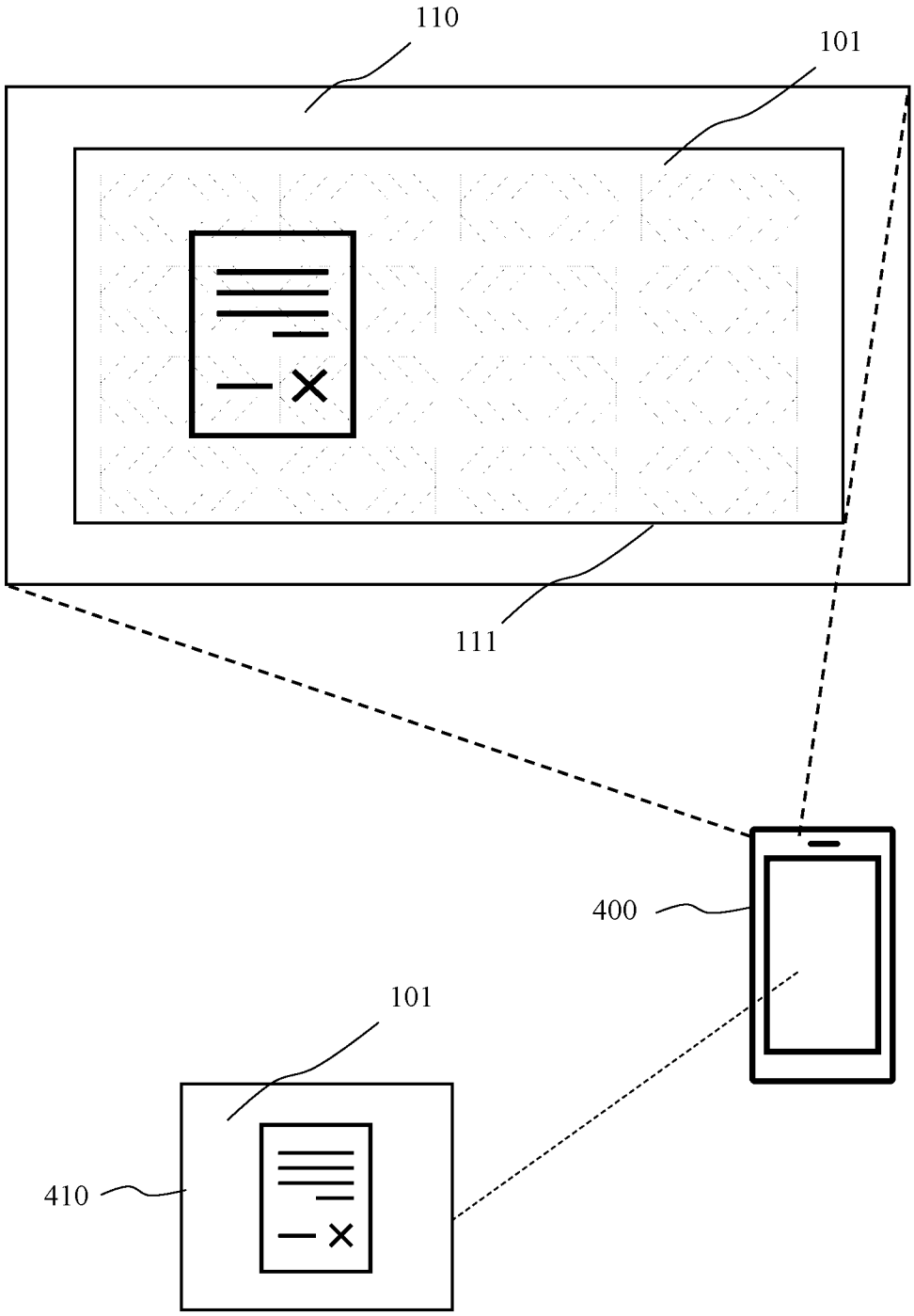
Фиг. 3А



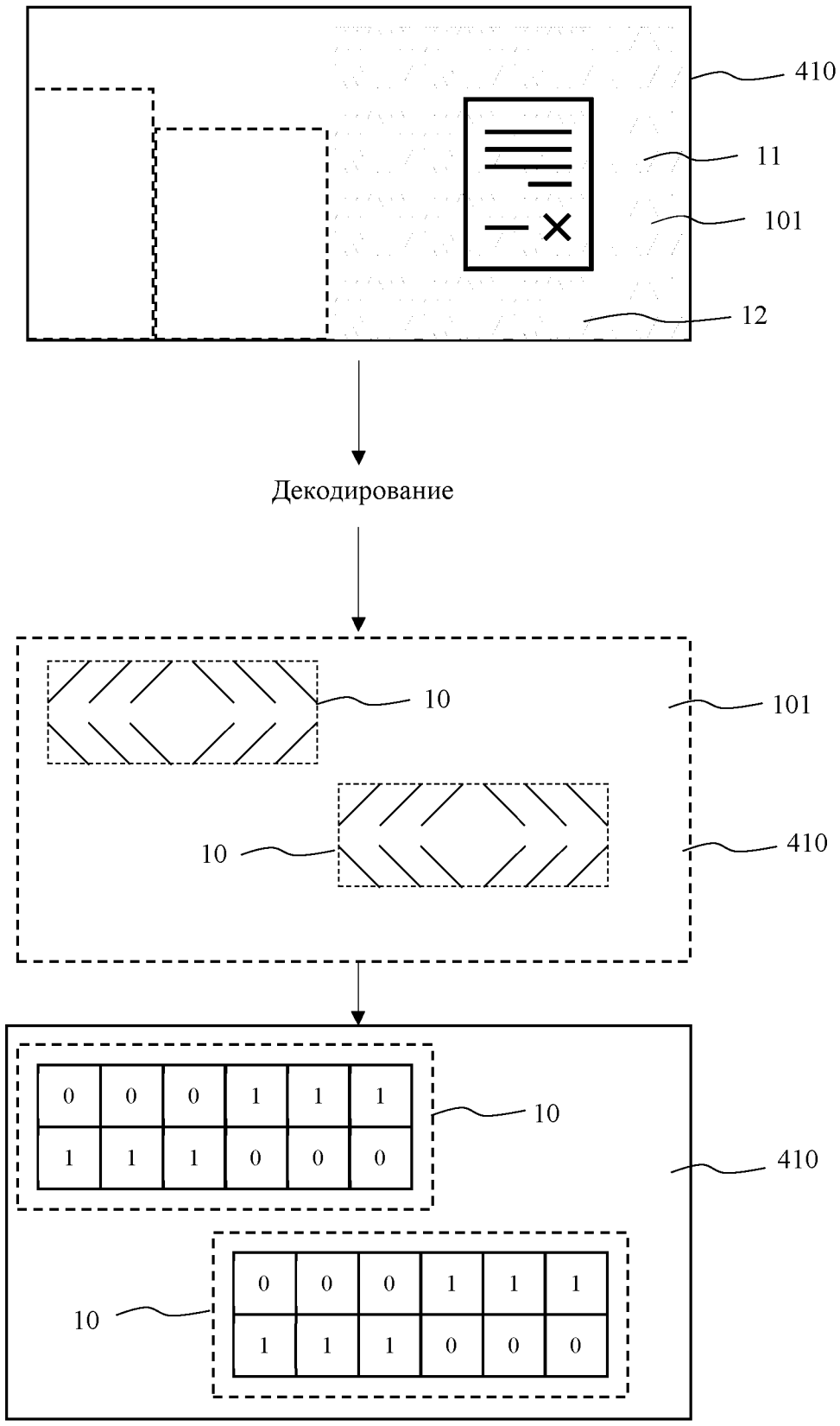
Фиг. 3Б


300
Получение изображения с информацией на экране ВУ
301
Декодирование информации
302
Попиксельное разложение на пороговые изображения
3021
Выявление графических элементов
3022
Восстановление информации из графических элементов
3023

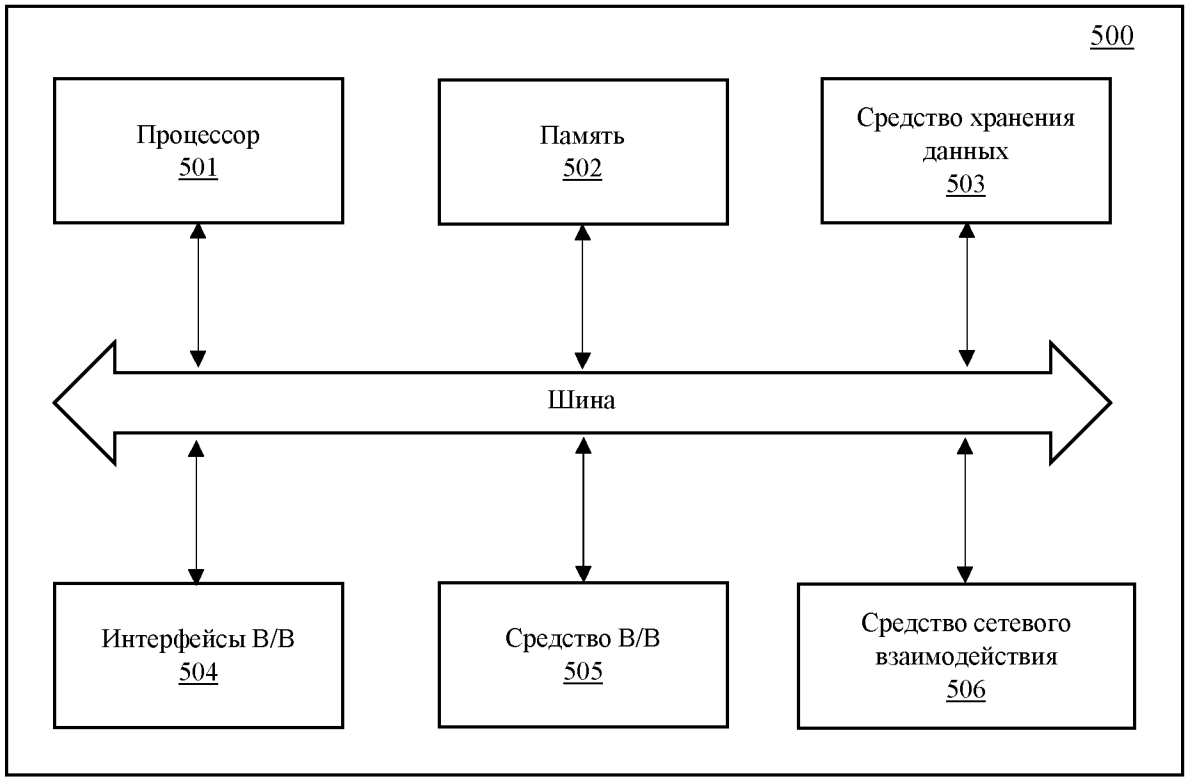
Фиг. 4



Фиг. 5


410
11
101
12
Декодирование
10
101
10
410
0 0 0 1 1 1
1 1 1 0 0 0
10
410
10
0 0 0 1 1 1
1 1 1 0 0 0

Фиг. 6


500
Процессор
501
Память
502
Средство хранения данных
503
Шина
Интерфейсы В/В
504
Средство В/В
505
Средство сетевого взаимодействия
506

Фиг. 7

ОТЧЕТ О ПАТЕНТНОМ ПОИСКЕ

(статья 15(3) ЕАПК и правило 42 Патентной инструкции к ЕАПК)

Номер евразийской заявки:

202191516

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:
G06F 21/16 (2013.01)
G06T 1/00 (2006.01)

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
G06F 1/00, 16/00-16/50, 17/00, 21/00-21/16, G06T 1/00, 7/00, H04N 21/43

Электронная база данных, использовавшаяся при поиске (название базы и, если, возможно, используемые поисковые термины)
Espacenet, ЕАПАТИС, EPOQUE Net, Reaxys, Google

В. ДОКУМЕНТЫ, СЧИТАЮЩИЕСЯ РЕЛЕВАНТНЫМИ

Категория*	Ссылки на документы с указанием, где это возможно, релевантных частей	Относится к пункту №
A	US 2017/0068829 A1 (AIRWATCH LLC) 09.03.2017	1-15
A	US 2010/0177977 A1 (GOOGLE INC) 15.07.2010	1-15
A	US 2009/0080689 A1 (JIAN ZHAO et al.) 26.03.2009	1-15
A	RU 2434356 C2 (ТОМСОН ЛАЙСЕНСИНГ) 20.11.2011	1-15
A	US 2010/0226572 A1 (MITSUMI ELECTRIC CO., LTD et al.) 09.09.2010	1-15
A	WO 2015/156640 A1 (SAMSUNG ELECTRONICS CO., LTD) 15.10.2015	1-15
A	US 2011/0188700 A1 (KT CORPORATION) 04.08.2011	1-15
A	US 2010/0064305 A1 (DOLBY LABORATORIES LICENSING CORPORATION) 11.03.2010	1-15

☐ последующие документы указаны в продолжении

* Особые категории ссылочных документов:
«A» - документ, определяющий общий уровень техники
«D» - документ, приведенный в евразийской заявке
«E» - более ранний документ, но опубликованный на дату подачи евразийской заявки или после нее
«O» - документ, относящийся к устному раскрытию, экспонированию и т.д.
"P" - документ, опубликованный до даты подачи евразийской заявки, но после даты испрашиваемого приоритета"

«T» - более поздний документ, опубликованный после даты приоритета и приведенный для понимания изобретения
«X» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий новизну или изобретательский уровень, взятый в отдельности
«Y» - документ, имеющий наиболее близкое отношение к предмету поиска, порочащий изобретательский уровень в сочетании с другими документами той же категории
«&» - документ, являющийся патентом-аналогом
«L» - документ, приведенный в других целях

Дата проведения патентного поиска: 06 апреля 2022 (06.04.2022)

Уполномоченное лицо:
Заместитель начальника Управления экспертизы - начальник отдела формальной экспертизы

Документ подписан электронной подписью
Сертификат: 1623340346878
Владелец: CN=Рогожин Д.Ю.
Действителен: 10.06.2021-09.06.2026

Д.Ю. Рогожин