(19) Евразийское патентное ведомство

(21) 202191517 (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)

(54) СПОСОБ И СИСТЕМА ЗАЩИТЫ ЦИФРОВОЙ ИНФОРМАЦИИ, ОТОБРАЖАЕМОЙ НА ЭКРАНЕ ЭЛЕКТРОННЫХ УСТРОЙСТВ

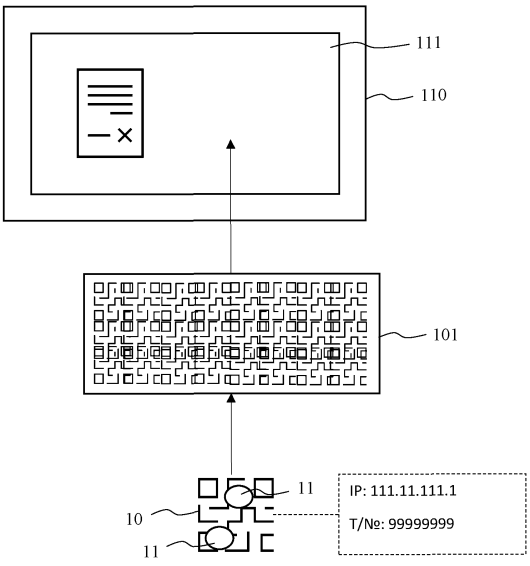
(31) **2021107968**
(32) **2021.03.25**
(33) **RU**

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

(72) Изобретатель:
Анистратенко Михаил Артурович, Анистратенко Александр Артурович, Оболенский Иван Александрович, Борисов Дмитрий Алексеевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(57) Изобретение относится к области защиты цифровых данных, в частности конфиденциальной и чувствительной информации, отображаемой на экране электронного устройства, с помощью внедрения цифровых меток (ЦМ) (10). Технический результат заключается в повышении устойчивости защиты информации за счет фрактального принципа формирования 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 элемента графического интерфейса заданной битовой размерности, содержащую, по меньшей мере, данные, идентифицирующие ВУ и/или пользователя ВУ, и реперные точки (11); формируют прозрачный защитный слой (101), не воспринимаемый человеческим глазом, который сформирован путем размещения ЦМ (10) в виде фрактального узора, заполняющего все пространство экрана (111) ВУ (110); накладывают сформированный защитный слой (101) на изображение, отображаемое на экране (111) ВУ (110).



202191517 A1

202191517 A1

МПК: G06F21/16

СПОСОБ И СИСТЕМА ЗАЩИТЫ ЦИФРОВОЙ ИНФОРМАЦИИ, ОТОБРАЖАЕМОЙ НА ЭКРАНЕ ЭЛЕКТРОННЫХ УСТРОЙСТВ

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 такой технологии 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, заключающую в снижении устойчивости (робастности) метода защиты цифровых данных при их фиксации внешними средствами с различных ракурсов и качеством съемки, что критически влияет на последующее декодирование данных из цифровых меток.

[0007] Технический результат заключается в повышении эффективности защиты информации на экране устройств, за счет улучшения устойчивости распознавания внедряемых цифровых меток в виде фрактального паттерна, формирующего защитный о слой.

[0008] Заявленный результат достигается за счет осуществления компьютерно-реализуемого способа защиты данных, отображаемых на экране вычислительных устройств (ВУ), выполняемого с помощью процессора и содержащего этапы, на которых:

формируют цифровую метку (ЦМ) в виде элемента графического интерфейса заданной битовой размерности, содержащую по меньшей мере данные, идентифицирующие ВУ и/или пользователя ВУ, и реперные точки;

формируют прозрачный защитный слой, не воспринимаемый человеческим глазом, который сформирован путем размещения ЦМ в виде фрактального узора, заполняющего все пространство экрана ВУ;

накладывают сформированный защитный слой на изображение, отображаемое на экране ВУ.

[0009] В одном из частных примеров реализации способа ЦМ формируется с помощью кодирования в контрастных каналах по меньшей мере одной цветовой схемы.

[0010] В другом частном примере реализации способа фрактальный рисунок слоя формируется рекурсивным методом построения ЦМ.

[0011] В другом частном примере реализации способа ЦМ имеет по меньшей мере один уровень вложенности.

[0012] В другом частном примере реализации способа ЦМ дополнительно содержит информацию о времени.

[0013] В другом частном примере реализации способа данные, идентифицирующие пользователя, выбираются из группы: табельный номер, имя, фотография или их сочетания.

[0014] В другом частном примере реализации способа данные, идентифицирующие ВУ, выбираются из группы: IP-адрес, MAC-адрес, уникальный идентификатор или их сочетания.

[0015] Заявленный технический результат также достигается за счет компьютерно-реализуемого способа идентификации данных, защищенных с помощью вышеуказанного способа, который выполняется с помощью процессора и содержит этапы, на которых:
получают изображение, содержащее по меньшей мере часть информации, отображаемой на экране ВУ;
осуществляют предобработку полученного изображения, в ходе которого обрабатывает геометрию изображения, выполняют коррекцию каналов в по меньшей мере одной цветовой палитре;
осуществляют декодирование предобработанного изображения, в ходе которого выявляют реперные точки ЦМ и извлекают информацию из ЦМ.

[0016] В одном из частных примеров реализации способа на этапе обработки геометрии изображения выполняется его вращение и коррекция перспективы.

[0017] В другом частном примере реализации способа при коррекции перспективы выполняется попиксельная бинарная интерполяция каналов изображения по меньшей мере одной цветовой схемы и коррекция размера изображения для сохранения его пропорций.

[0018] В другом частном примере реализации способа изображение получают от внешнего устройства.

[0019] Каждый из вышеуказанных способов также может быть реализован с помощью компьютерной системы, содержащей по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их выполнении процессором осуществляют любой из вышеуказанных способов.

КРАТКОЕ ОПИСАНИЕ ЧЕРТЕЖЕЙ

[0020] Фиг. 1 иллюстрирует общий принцип заявленного решения.

[0021] Фиг. 2 иллюстрирует блок-схему заявленного способа защиты данных.

[0022] Фиг. 3А иллюстрирует пример фрактального защитного слоя.

[0023] Фиг. 3Б иллюстрирует пример размещения слоя на экране устройства.

[0024] Фиг. 4 иллюстрирует блок-схему способа декодирования информации из изображения, защищенного ЦМ.

[0025] Фиг. 5 иллюстрирует пример захвата изображения информации с экрана устройства.

[0026] Фиг. 6 иллюстрирует принцип декодирования ЦМ из изображения.

[0027] Фиг. 7 иллюстрирует общий вид вычислительного устройства.

ОСУЩЕСТВЛЕНИЕ ИЗОБРЕТЕНИЯ

[0028] 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, осуществляется с помощью внедрения ЦМ (10), в которую кодируется соответствующая информация для последующего установления места и ответственного лица по несанкционированному получению информации вне защищенного периметра инфраструктуры, например, с помощью ее фотографирования, видеосъемки или захвата (скриншот) изображения на экране ВУ внешними устройствами (смартфон, фотоаппарат и т.п.), в том числе с последующей распечаткой.

[0029] 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 двух контрастных цветов. 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).

[0030] ЦМ (10) представляет собой статический элемент графического интерфейса заданной битовой размерности. Помимо информации для идентификации факта фотографирования информации на экране (111) в ЦМ (10) внедряются также одна или несколько реперных точек (11), необходимых для последующей идентификации расположения ЦМ (10).

[0031] Далее из ЦМ (10) на этапе (202) формируют защитный слой (101) в виде фрактального принципа размещения ЦМ (10), заполняя все пространство экрана (111). Количество ЦМ (10) и принцип фрактального размещения определяется исходя из разрешающей способности экрана (111) и размерности ЦМ (10). Как правило, ЦМ (10) выбираются равной размерности, но могут также иметь чередующийся порядок из

размещения для формирования слоя (101), что также не нарушает техническое воплощение заявленного решения в части последующей идентификации данных.

[0032] Защитный слой (101) формируется невидимым (прозрачным), чтобы не быть различимым человеческим глазом и скрыть факт применения защиты данных на экране (111). Прозрачность слоя (101) создаваемого фрактального узора 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. 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.

[0033] 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.

[0034] На Фиг. 3А – 3Б представлен пример сформированного защитного слоя (101) на основе множества ЦМ (10) с соответствующим размещением реперных точек (11). Представленный пример ЦМ (10) может создаваться с применением кодирования информации в контрастных каналах цветовой схемы, например, RGB, HSL, ARGB и т.п. Фрактальная конструкция рисунка слоя (101) может формироваться рекурсивным методом построения (размещения) ЦМ (10) и иметь один или несколько уровней вложенности (рекурсии) ЦМ (10) друг в друга.

[0035] Как указывалось выше, на примере, приведенным на Фиг. 3А, при формировании ЦМ (10) применяются два контрастных цвета, один из которых представляет собой фон ЦМ (10) – логический 0, а второй – контрастный от цвета фона, представляющий логическую 1. Создание защитного слоя (101) начинается с 0-го уровня рекурсии, на котором фон ЦМ (10) выбирается большим по размеру чем отображаемая область (111) на экране (110). После этого начинается цикл рекурсии, в ходе которого определяется размер прямоугольника, описывающего один бит ЦМ (10) (далее – битовый прямоугольник), в соответствии с системой уравнений:

$$\begin{cases} xy = lx'y' \\ \dfrac{x}{y} = \dfrac{x'}{y'} \end{cases}$$

Где: x-длина фона ЦМ, y- ширина фона ЦМ, x'-длина битового прямоугольника, y'-ширина битового прямоугольника, l-длина битового массива кодируемого сообщения.

[0036] Далее ЦМ (10) начинает заполняться битовыми прямоугольниками, где, как указывалось выше, 0 – цвет прямоугольника аналогичный фону метки, 1 – цвет прямоугольника контрастный фону метки. Осуществляется заполнение ЦМ (10) всеми битами (по всему фону ЦМ) в ходе чего формируется метка n-го уровня. Цикл рекурсии повторяется заново, за следующий размер ЦМ (10) берется один битовый прямоугольник текущей ЦМ (10). Цикл повторяется до тех пор, пока размер ЦМ (10) не будет равен 1x1 пиксель. ЦМ (10) в виде битовых прямоугольников перебираются до тех пор, пока все ЦМ (10) на всех уровнях рекурсии не достигнут конца рекурсии.

[0037] Далее рассмотрим процесс декодирования информации, защищенной ЦМ, представленной на Фиг. 4 – Фиг. 6. Фиг. 4 иллюстрирует блок-схему выполнения способа (400) декодирования информации из захватываемого изображения.

[0038] 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.

[0039] Далее полученное изображение (410) проходит этап обработки (302), в ходе которого осуществляется геометрическое преобразование изображения, в частности вращение и/или коррекция перспективы. Коррекция перспективы производится в два этапа – попиксельная бинарная интерполяция цветовых каналов изображения (например, RGB) для изменения перспективы изображения и коррекция размера изображения для сохранения пропорций по формуле:

$$targetWidth = \frac{topWidth + bottomWidth}{2} + 2 \cdot deltaX;$$

$$targetHeight = \frac{leftHeight + rightHeight}{2} + 2 \cdot deltaY,$$

Где:

deltaX – длина горизонтальной проекции отрезка между точками пересечения диагоналей четырехугольника и его центроидом,

deltaY – длина вертикальной проекции отрезка между точками пересечения диагоналей четырехугольника и его центроидом,

topWidth – длина горизонтальной проекции верхней грани четрехугольника,

bottomWidth – длина горизонтальной проекции нижней грани четырехугольника,

leftHeight - длина вертикальной проекции левой грани четырехугольника,

rightHeight – длина вертикальной проекции правой грани четырехугольника.

[0040] Далее производится изменение цветности/насыщенности (saturation) полученного изображения по меньшей мере в одной цветовой палитре для повышения контрастности изображения в целом и выявления присутствия ЦМ (10) на том или ином участке изображения (410).

[0041] После этого осуществляется взаимная коррекция цветовых каналов полученного изображения (410) для выделения контрастных цветов, выбранных при кодировании ЦМ (10). Выполняется удаление одного из контрастных цветов, выбранного при кодировании ЦМ (10), в каждом пикселе полученного изображения.

[0042] На этапе (303) положение ЦМ (10) определяется с помощью реперных точек (11), выявленных на изображении (410). Определяются центры реперных точек (11), вокруг которых строится окружность заданного радиуса, вычисляемого из радиуса реперных точек и длины закодированного сообщения, на периметре которой определяются центры других реперных точек (11). Из угла отрезка между двумя центрами к горизонтали и длины этого отрезка вычисляются угол наклона и размер ЦМ (10) соответственно.

[0043] Из известной длины сообщения и известного размера ЦМ (10) вычисляется размер битового прямоугольника ЦМ (10).

[0044] Как представлено на Фиг. 6 в результате декодирования предобработанного изображения (410) определяются ЦМ (10) на защитном слое (101) на всех уровнях рекурсии (в зависимости от качества входного изображения).

[0045] Этапы (302) – (303) выполняются несколько раз при разных параметрах изменения насыщенности и изменении цветов. Результатом берутся значения, которые наиболее часто повторяются при разных параметрах. Это обеспечивает надежное декодирование цвета каждого пикселя полученного изображения в соответствии с законами нормального распределения при различных параметрах коррекции.

[0046] После надежного определения цвета каждого пикселя в полученном изображении (410) по цвету реперных точек (11) определяется цвет фона данной ЦМ, а по цвету реперной точки ЦМ, вписанной в битовый прямоугольник данной ЦМ, определяется цвет данного битового прямоугольника. Обладая информацией о цвете каждого битового прямоугольника в данной ЦМ и цвете фона данной ЦМ, производится построение битового массива закодированного сообщения.

[0047] Из битового массива закодированного сообщения, зная алгоритм кодирования данного сообщения, производится преобразование битового массива в полезную информацию, закодированную в ЦМ.

[0048] Данный принцип защиты и последующего декодирования информации из защитного слоя (101) позволяет более эффективно распознать закодированную информацию из ЦМ (10) и установить ВУ (110) и/или лицо, ответственное за утечку конфиденциальной и/или чувствительной информации.

[0049] 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.

[0050] 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).

[0051] 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.

[0052] 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.).

[0053] 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.

[0054] Для организации работы компонентов устройства (500) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (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.

[0055] Для обеспечения взаимодействия пользователя с вычислительным устройством (500) применяются различные средства (505) В/В 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.

[0056] 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.

[0057] Дополнительно могут применяться также средства спутниковой навигации в составе устройства (500), например, GPS, ГЛОНАСС, BeiDou, Galileo.

[0058] 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 вычислительных устройств (ВУ), выполняемый с помощью процессора и содержащий этапы, на которых:

- формируют цифровую метку (ЦМ) в виде элемента графического интерфейса заданной битовой размерности, содержащую по меньшей мере данные, идентифицирующие ВУ и/или пользователя ВУ, и реперные точки;
- формируют прозрачный защитный слой, не воспринимаемый человеческим глазом, который сформирован путем размещения ЦМ в виде фрактального узора, заполняющего все пространство экрана ВУ;
- накладывают сформированный защитный слой на изображение, отображаемое на экране ВУ.

2. Способ по п.1, характеризующийся тем, что ЦМ формируется с помощью кодирования в контрастных каналах по меньшей мере одной цветовой схемы.

3. Способ по п.1, характеризующийся тем, что фрактальный рисунок слоя формируется рекурсивным методом построения ЦМ.

4. Способ по п.1, характеризующийся тем, что ЦМ имеет по меньшей мере один уровень вложенности.

5. Способ по п.1, характеризующийся тем, что ЦМ дополнительно содержит информацию о времени.

6. Способ по п.1, характеризующийся тем, что данные, идентифицирующие пользователя, выбираются из группы: табельный номер, имя, фотография или их сочетания.

7. Способ по п.1, характеризующийся тем, что данные, идентифицирующие ВУ, выбираются из группы: IP-адрес, MAC-адрес, уникальный идентификатор или их сочетания.

8. Компьютерно-реализуемый способ идентификации данных, защищенных с помощью способа по любому из пп. 1-7, выполняемый с помощью процессора и содержащий этапы, на которых:

- получают изображение, содержащее по меньшей мере часть информации, отображаемой на экране ВУ;
- осуществляют предобработку полученного изображения, в ходе которого обрабатывает геометрию изображения, выполняют коррекцию каналов в по меньшей мере одной цветовой палитре;

– осуществляют декодирование предобработанного изображения, в ходе которого выявляют реперные точки ЦМ и извлекают информацию из ЦМ.

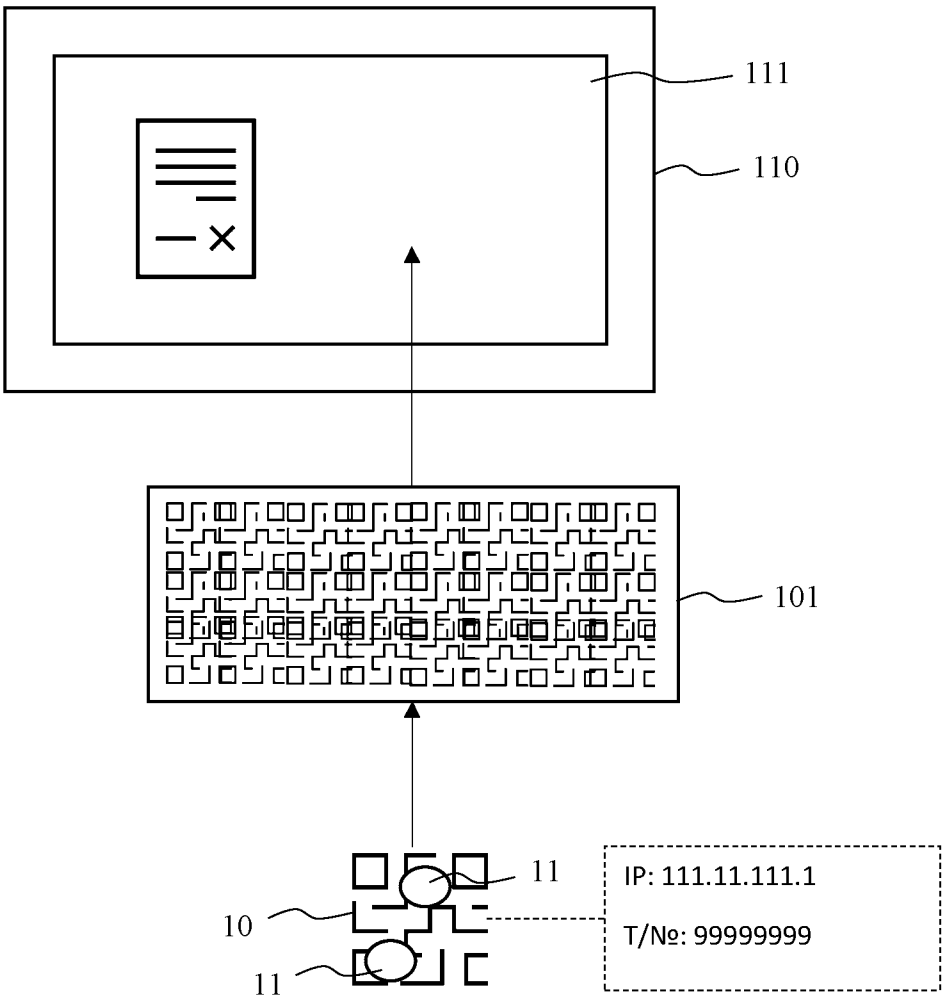
9. Способ по п.8, характеризующийся тем, что на этапе обработки геометрии изображения выполняется его вращение и коррекция перспективы.

10. Способ по п.9, характеризующийся тем, что при коррекции перспективы выполняется попиксельная бинарная интерполяция каналов изображения по меньшей мере одной цветовой схемы и коррекция размера изображения для сохранения его пропорций.

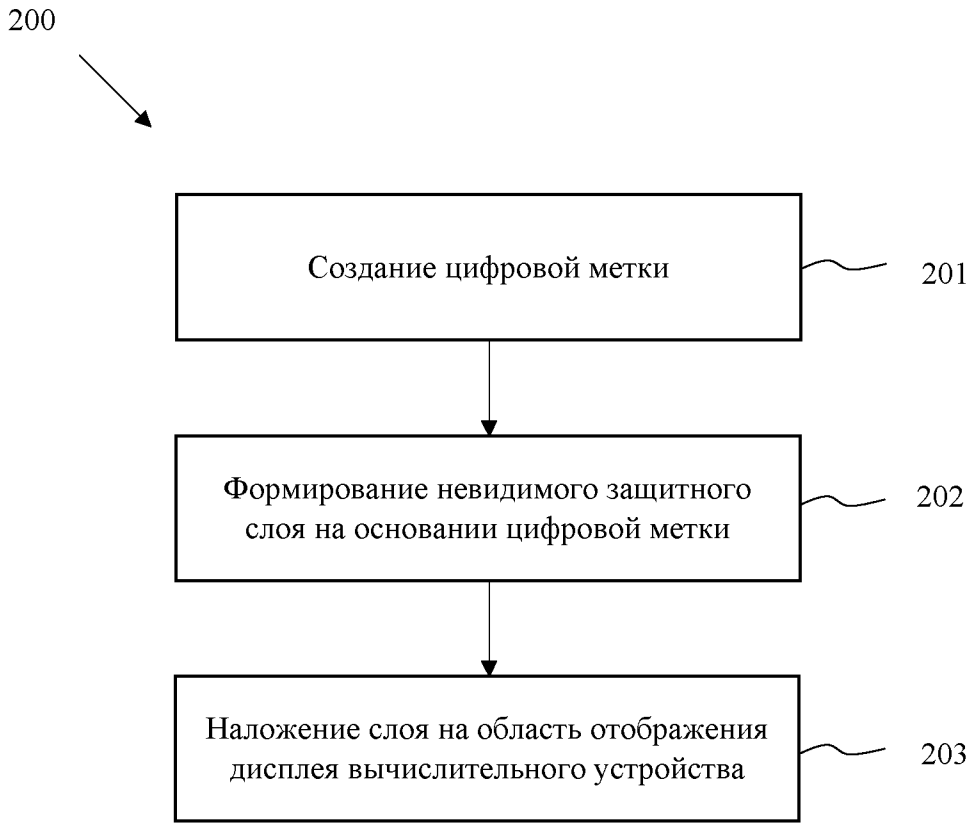
11. Способ по п.8, характеризующийся тем, что изображение получают от внешнего устройства.

12. Система защиты данных, отображаемых на экране ВУ, содержащая по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их выполнении процессором осуществляют способ по любому из пп. 1-7.

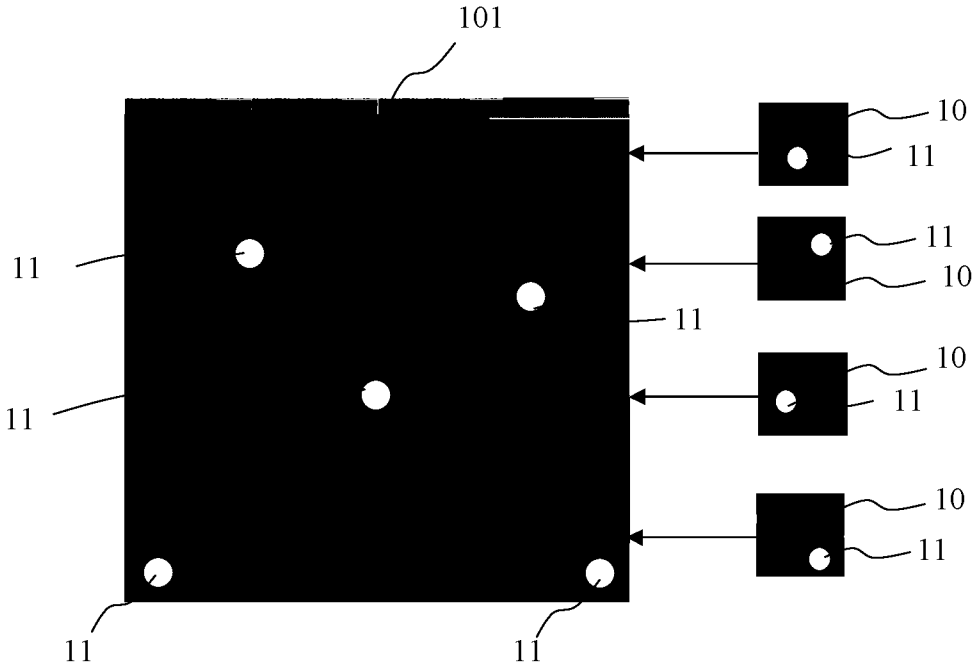
13. Система идентификации данных, отображаемых на экране ВУ, содержащая по меньшей мере один процессор и по меньшей мере одну память, хранящую машиночитаемые инструкции, которые при их выполнении процессором осуществляют способ по любому из пп. 9-11.



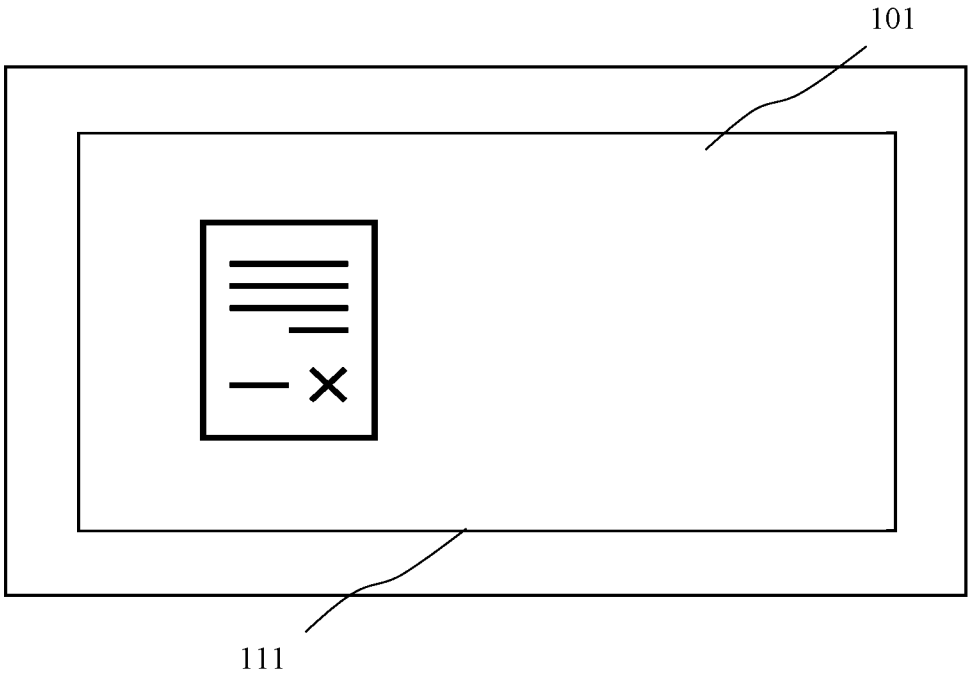
Фиг. 1


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

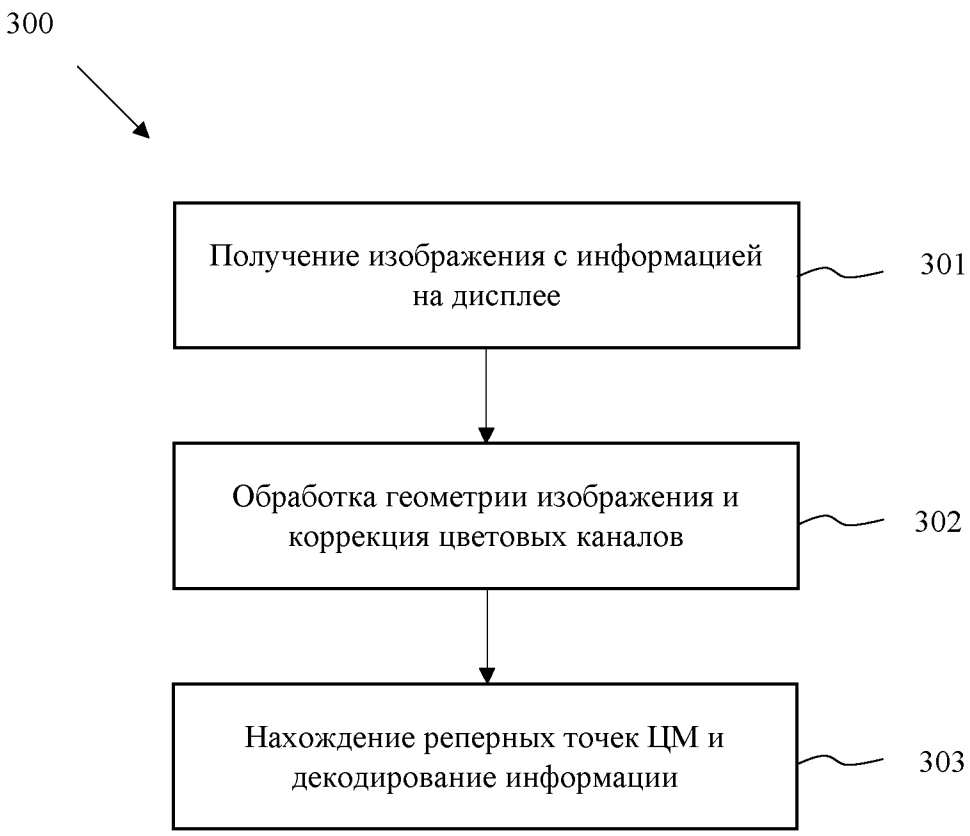
Фиг. 2



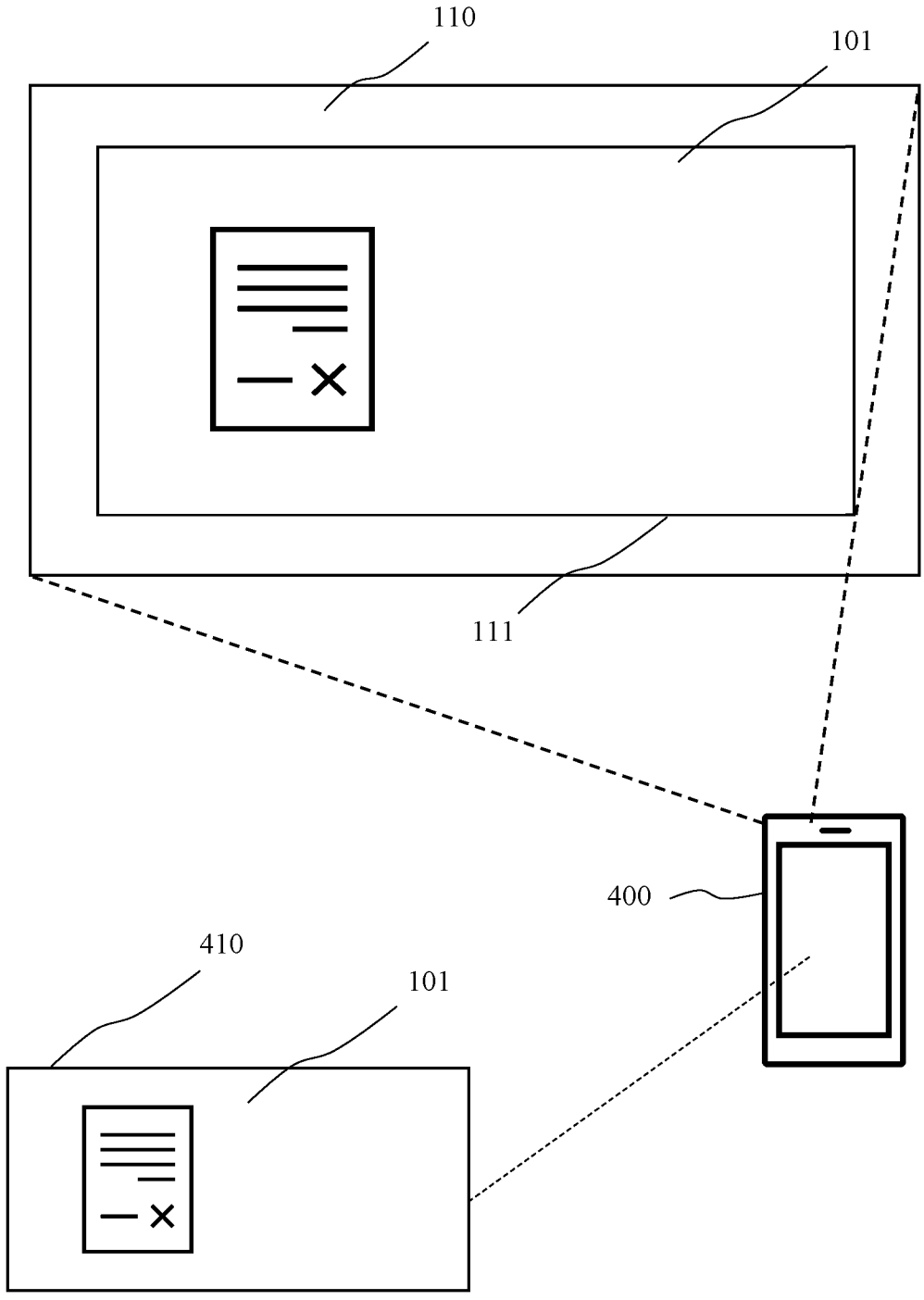
Фиг. 3А



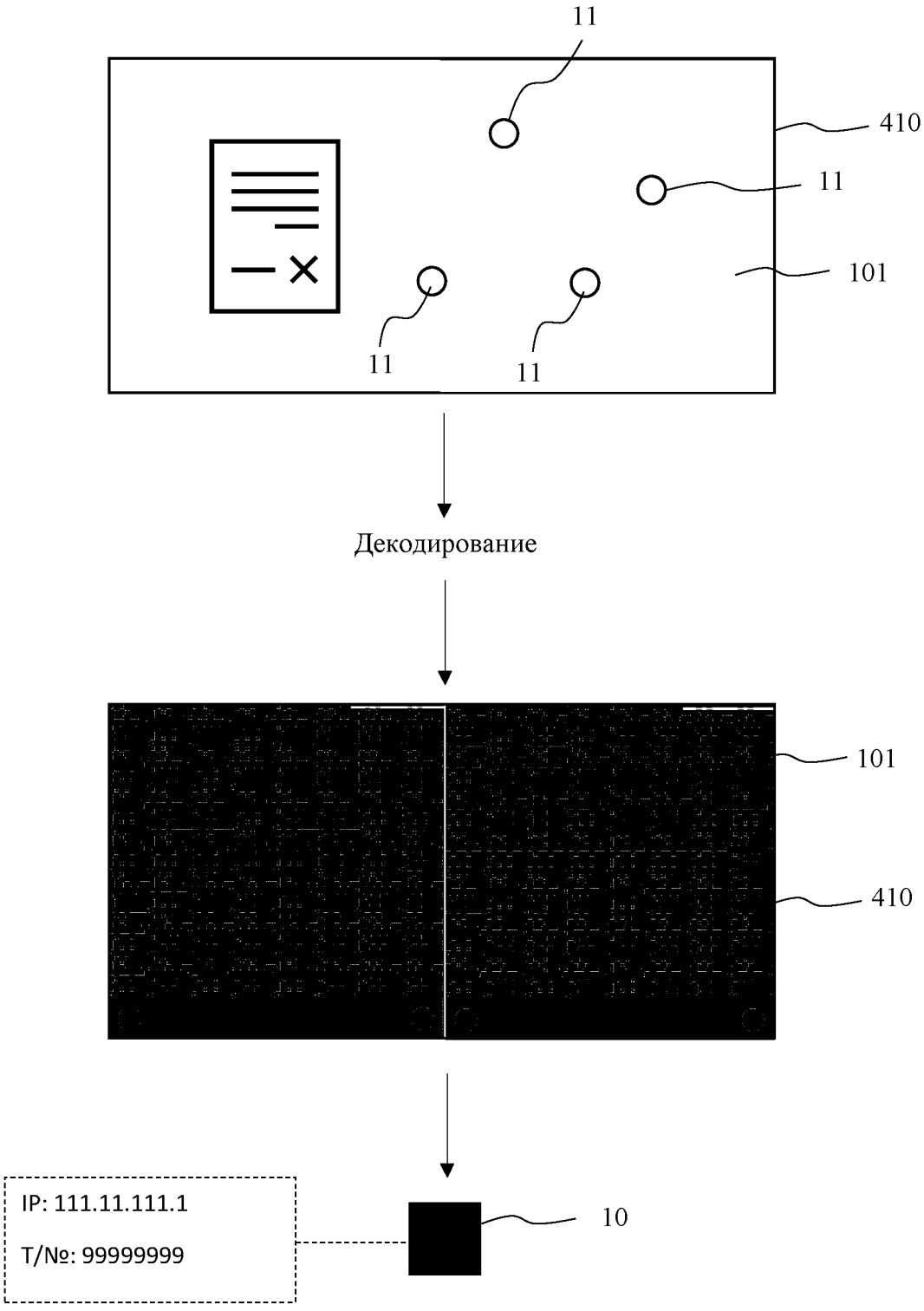
Фиг. 3Б


300
Получение изображения с информацией на дисплее
301
Обработка геометрии изображения и коррекция цветовых каналов
302
Нахождение реперных точек ЦМ и декодирование информации
303

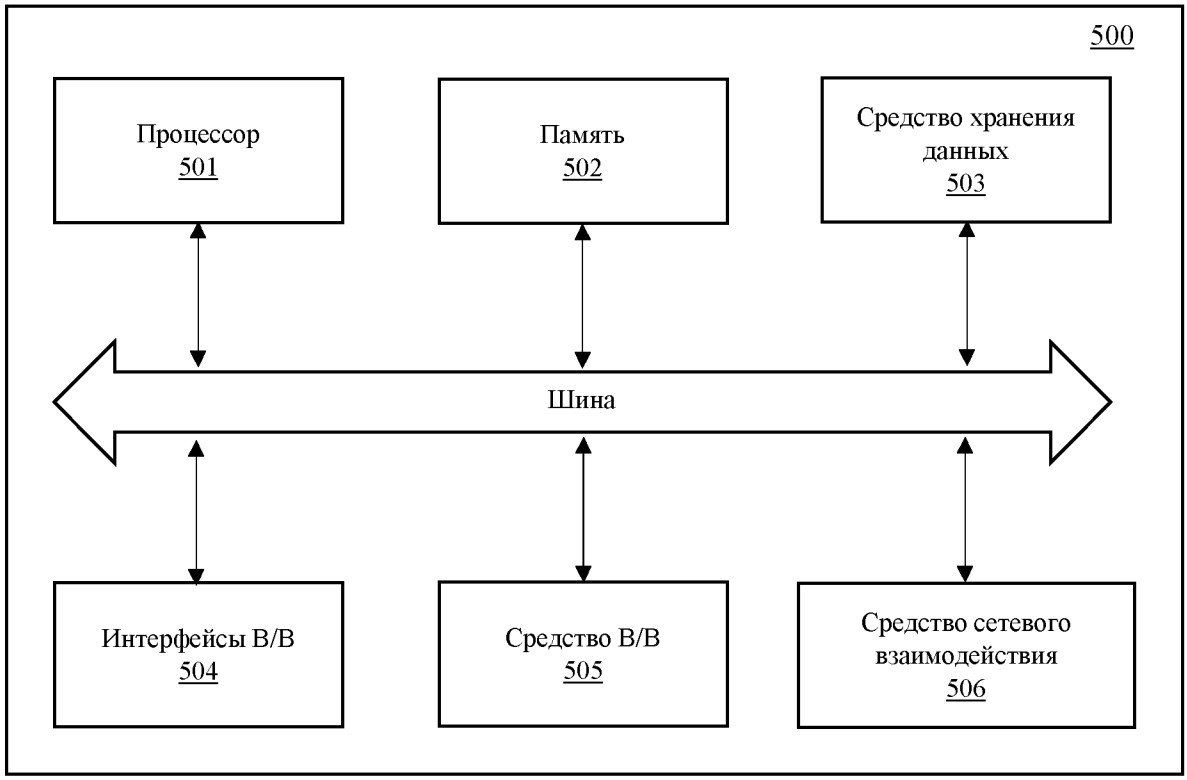
Фиг. 4



Фиг. 5


11
410
11
101
11
11
Декодирование
101
410
IP: 111.11.111.1
T/№: 99999999
10

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:

202191517

А. КЛАССИФИКАЦИЯ ПРЕДМЕТА ИЗОБРЕТЕНИЯ:
G06F 21/16 (2013.01)

Согласно Международной патентной классификации (МПК)

Б. ОБЛАСТЬ ПОИСКА:

Просмотренная документация (система классификации и индексы МПК)
G06F 21/00, 21/10, 21/16, 21/60, 12/00, 12/14, G06T 1/00, H04N 1/00, 19/46, 19/467, 21/00, 21/80, 21/83, 21/835, 21/8358, 7/00, 5/00, 5/76, 5/91, 5/913, H04L 9/00, G06K 9/00, 7/00, 7/10

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, D	US 9239910 B2 (MARKANY INC.) 19.01.2016, реферат, колонка 5, строка 22-колонка 6, строки 27, 62-колонка 7, строка 3, колонка 9, строки 39-46, колонка 10, строка 56-колонка 11, строка 11, фигуры 2, 4	1-13
A	US 2016/0162716 A1 (AI CURE TECHNOLOGIES, INC.) 09.06.2016, параграфы [0032], [0034]-[0035], [0038], [0119], [0136]-[0137], [0229]-[0236], фигуры 10, 14-15	1-13
A	RU 82398 U1 (БАЙЧУРИН ЮЛАЙ ХАКИМОВИЧ) 20.04.2009	1-13
A	US 7269734 B1 (DIGIMARC CORPORATION) 11.09.2007	1-13
A	RU 2424554 C2 (ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ УЧРЕЖДЕНИЕ "ГОСУДАРСТВЕННЫЙ НАУЧНО-ИССЛЕДОВАТЕЛЬСКИЙ ИСПЫТАТЕЛЬНЫЙ ИНСТИТУТ ПРОБЛЕМ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ"), 20.07.2011	1-13
A	US 8406459 B2 (GEMALTO SA ert al) 26.03.2013	1-13

☐ 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: 15 апреля 2022 (15.04.2022)

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