(19) Евразийское патентное ведомство

(11) 039818 (13) B1

(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ

(45) Дата публикации и выдачи патента
2022.03.16

(21) Номер заявки
202092874

(22) Дата подачи заявки
2020.12.23

(51) Int. Cl. ***H04L 9/00*** (2006.01)

(54) СПОСОБ СТЕГАНОГРАФИРОВАНИЯ ЦИФРОВОГО ИЗОБРАЖЕНИЯ С ПОМОЩЬЮ ГРАФИЧЕСКОЙ ЦИФРОВОЙ МЕТКИ И СПОСОБ ДЕШИФРОВАНИЯ СТЕГАНОГРАФИРОВАННОГО ИЗОБРАЖЕНИЯ

(31) **2020136300**
(32) **2020.11.05**
(33) **RU**
(43) **2022.03.15**

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

(72) Изобретатель:
Крамаренко Сергей Михайлович, Сысоев Валентин Валерьевич (RU)

(74) Представитель:
Герасин Б.В. (RU)

(56) US-A1-20040025025
US-A1-20050129269
US-5687236

(57) Представленное решение позволяет защищать цифровую фотографию от неправомерного использования путем нанесения цифровой метки, таким образом, чтобы наличие цифровой метки было неизвестно пользователю, было достаточно труднообнаружимо для стегоаналитика и выдерживало ряд атак, к примеру, вырезание части изображения, изменение яркостных и контрастных характеристик, ухудшение качества самого изображения, атаку белым шумом. Заявленный результат достигается за счет компьютерно-реализуемого способа математической аппроксимации нанесения на изображения безлинзовой голограммы Фурье, где в качестве самой голограммы выступает само изображение.

039818 B1

039818 B1

Область техники

Представленное техническое решение относится к области кодирования и декодирования данных, а в частности к способу и устройству внесения цифровых меток в цифровое изображение.

Уровень техники

Проблема защиты авторского или эксклюзивного права на информацию является на сегодняшний день является актуальной в коммерческих и государственных организациях, в связи с чем постоянно предлагаются новые подходы в области защиты данных, в целях противодействия неправомерному использованию, краже или утечке данных. Несанкционированное/неправомерное применение данной информации может приводить для организаций как к репутационному ущербу (судебные иски, претензии, негативный опыт и отток клиентов, разрыв отношений с подрядчиками и партнерами), так и к прямым финансовым убыткам (штрафы регуляторов, компенсации клиентам и контрагентам, потеря доли рынка, недополучение прибыли в следствии приостановления/прекращения деятельности из-за отзыва лицензий и т.п.). Одним из примеров применяемых подходов является стеганографирование изображения (https://ru.\wikipedia.org/wiki/Стеганография). Стеганография - это способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи (хранения), т.е. защищенное изображение фактически неотличимо от оригинала. Цифровая стеганография - направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, вызывая при этом некоторые искажения этих объектов, например, цифровые метки (ЦМ) или цифровые водяные знаки (ЦВЗ). Как правило, данные объекты являются мультимедиа-объектами (изображения, видео, аудио, текстуры 3D-объектов) и внесение искажений, которые находятся ниже порога чувствительности среднестатистического человека, не приводит к заметным изменениям этих объектов.

Для повышения устойчивости к искажениям часто применяют помехоустойчивое кодирование или используют широкополосные сигналы. Создаваемый водяной знак внедряется в контейнер, например, используются особенности восприятия изображений человеческим глазом, путём изменения младших значащих бит, или по другим алгоритмам, использующих особенности формата, в котором представлен контейнер (алгоритмы JSteg, F5).

Так же, используются методы, учитывающие при внедрении ЦВЗ особенности восприятия изображений человеческим глазом. Известно, что изображения имеют огромную психовизуальную избыточность. Глаза человека подобны низкочастотному фильтру, который игнорирует мелкие элементы изображения. Таким образом, добавляя в изображение в случайном порядке точки, можно добиться сокрытия в изображении ЦВЗ (алгоритм Patchwork).

Примеры такого подхода известен, например, из патента США 10,560,599 B2 (Digimarc Corp, 11.02.2020). Известный способ основывается на внедрении ЦМ в изображение для последующего репродуцирования, например, печати, с помощью анализа интенсивности/силы сигнала и внедрении ЦМ на основании вычисленного сигнала. Недостатком данного подхода является недостаточная стойкость зашифрованного изображения, что позволяет с помощью применения тех или иных видов атак, например, наложением белого шума на изображение, разрушить внедренную ЦМ.

Сущность изобретения

Заявленным решением предлагается новый подход в решении существующей технической проблемы, заключающийся в более защищенном методе стеганографирования изображений.

Техническим результатом является повышение эффективности защиты изображений, за счет автоматизированного внедрения цифровых меток, содержащей закодированную информацию на основании хеш-суммы входного изображения, подтверждающую аутентичность изображения.

Заявленный результат достигается за счет компьютерно-реализуемого способа стеганографирования цифрового изображения с помощью графической цифровой метки (далее - ЦМ), выполняемый с помощью по меньшей мере одного процессора и содержащий этапы, на которых:

a) получают по меньшей мере одно входное изображение;

b) формируют хеш-сумму упомянутого входного изображения;

c) осуществляют шифрование полученной хеш-суммы;

d) создают контрольную сумму на основании зашифрованной хеш-суммы изображения;

e) формируют кортеж данных, состоящий из полученных хеш-суммы и контрольной суммы;

f) на основе полученного кортежа формируют ЦМ в виде цифрового изображения, содержащего данные в графическом представлении;

g) формируют матрицу значений яркости пикселей графической ЦМ путем выполнения следующих этапов:

осуществляют попиксельный перевод изображения ЦМ из RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей изображения ЦМ (I_m),

в матрице значений яркостей пикселей изображения ЦМ (I_m) производят округление значений, лежащих в диапазоне от 0 до 1 в большую или меньшую сторону;

h) формируют матрицу комплексных чисел от значений яркости пикселей входного цифрового изображения путем выполнения следующих этапов:

осуществляют попиксельный перевод входного цифрового изображения из RGB в цветовое про-

странство HSV с последующим построением матрицы значений яркостей пикселей изображения (I_p), и формированием матриц значений тона (H_p) и насыщенности (S_p) пикселей изображения в цветовом пространстве HSV;

формируют кортеж $K(I_p)$ из значений яркостей пикселей путем построчного перевода из полученной матрицы значений яркостей пикселей (I_p); формируют кортеж комплексных чисел $K(I_f)$ с помощью применения к кортежу яркостей прямого дискретного быстрого преобразование Фурье (ДБПФ);

формируют матрицу комплексных чисел (I_f) из кортежа комплексных чисел $K(I_f)$ той же размерности, что и матрица значений яркостей пикселей (I_p) полученной на этапе 1);

i) создают промежуточную матрицу стеганограммы (I_o) с помощью сложения матриц, полученных на этапе h) и g), причем осуществляют сложение матрицы значений яркости пикселей графической ЦМ (I_m) и матрицы комплексных чисел от значений яркости пикселей входного цифрового изображения (I_f);

j) из промежуточной матрицы стеганограммы (I_o), полученной на этапе i), формируют матрицу яркостей пикселей стеганограммы (I*) посредством быстрого обратного дискретного преобразования Фурье (ДБПФ);

k) формируют матрицу, содержащую все три значения (H_p, S_p, I*) цветового пространства HSV, описывающую стеганографированное цифровое изображение, в котором значения ячеек из матрицы яркости пикселей стеганограммы (I*), полученной на этапе j) объединены со значениями матриц тонов (H_p) и значений насыщенностей (S_p) входного цифрового изображения, полученных на этапе h); l) на основе матрицы, полученной на этапе k) воспроизводят стеганографированное цифровое изображение посредством перевода каждой ячейки упомянутой матрицы (H_p, S_p, I*) из цветового пространства HSV в цветовое пространство RGB.

В одном из частных примеров осуществления способа шифрование хеша осуществляется с применением ассиметричных криптографических алгоритмов на приватном ключе.

В другом частном примере осуществления способа данные, формирующие ЦМ, могут быть представлены в графическом виде и/или в виде буквенно-символьной последовательности.

В другом частном примере осуществления способа размер цифрового изображения ЦМ для нанесения на входное изображение определяется на основании размера шрифта, используемого при подготовке кортежа данных.

В другом частном примере осуществления способа размер ЦМ не превышает 1/8 размера входного цифрового изображения.

В другом частном примере осуществления способа слой является черным, а буквенно-символьный кортеж данных, несущий семантику ЦМ, наносится в белом цвете. В другом частном примере осуществления способа значения яркостей пикселей входного цифрового изображения (I) построчно переводятся в матрицу яркостей K[I] исходя из фактического размера изображения в пикселях.

В другом частном примере осуществления способа хеш-сумма формируется с помощью преобразования в массив байт и применения алгоритма хеширования. В другом частном примере осуществления способа алгоритм хеширования выбирается из группы: MD2/4/5/6, SHA, SHA224, SHA256, SHA384, SHA512, ГОСТ 34.11-94.

В другом частном примере осуществления способа ЦМ размещается в одном из четырех возможных квадрантов изображения, условно разделенного на четыре равных фрагмента.

В другом частном примере осуществления способа на этапе g) дополнительно выполняется формирование матриц значений тона (H_m) и насыщенности (S_m).

В другом частном примере осуществления способа на этапе h) кортеж комплексных чисел K(I*) формируется с помощью преобразования, обеспечивающего перевод рациональных значений в комплексные значения, при этом преобразование выбирается из группы: прямое/обратное преобразование Фурье, прямое/обратное дискретное быстрое преобразование Фурье (ДБПФ), косинусное преобразование, преобразование Адамара (Уолша-Адамара), преобразование Френеля. Заявленное техническое решение осуществляется также за счет выполнения компьютерно-реализуемого способа дешифрования цифровых изображений, стеганографированных с помощью вышеуказанного способа, выполняемого с помощью процессора и содержащего этапы, на которых:

a) получают входной стегоконтейнер, содержащий цифровое изображение, в котором закодированы данные ЦМ;

b) формируют матрицу комплексных чисел стегоконтейнера (I), с помощью выполнения следующих этапов:

1) осуществляют перевод изображения входного стегоконтейнера из RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей (I_k);

2) формируют кортеж K(I) из значений яркостей пикселей путем построчного перевода из полученной матрицы значений яркостей пикселей (I_k);

3) формируют кортеж комплексных чисел K(I*) значений яркости посредством быстрого обратного дискретного преобразования Фурье (ДБПФ);

4) формируют матрицу комплексных чисел (I*) из кортежа комплексных чисел K(I*) той же размерности, что и матрица значений яркостей пикселей (I_k), полученная на шаге 1);

5) рассчитывают матрицу значений яркостей пикселей стегоконтейнера (I) с помощью вычисления абсолютных значений комплексных чисел в каждой ячейки матрицы комплексных чисел (I*), полученной на предыдущем шаге;

c) определяют в матрице значений яркостей пикселей (I_k) подматрицу яркостей (I_r), в которой размещена ЦМ;

d) на основании подматрицы яркостей (I_r) осуществляют считывание и распознавание фрагмента изображения, содержащего закодированную ЦМ;

e) разделяют данные ЦМ на зашифрованные данные и контрольную сумму;

f) выполняют расчет и сверку контрольной суммы от зашифрованных данных с извлеченной из цифрового изображения стегоконтейнера контрольной суммой;

g) выполняют дешифрование зашифрованной части ЦМ посредством открытого ключа.

В одном из частных примеров осуществления способа при выполнении этапа d) в тех ячейках матрицы, в которых присутствуют значения яркости выше среднего арифметического значения яркости всей матрицы, выполняется замена данных значений на нулевые.

В другом частном примере осуществления способа на этапе e) уменьшение зернистости осуществляется с помощью обнуления ячеек матрицы, у которых значения соседних ячеек близки или равны 0.

В другом частном примере осуществления способа при выполнении этапа f) в цветовом пространстве HSV монохромное полутоновое изображение получается путем использования яркости пикселя (I_r) из ячейки подматрицы, а насыщенность (S) и тон (H) принимают равными нулю.

В другом частном примере осуществления способа полученное монохромное полутоновое изображение переводится из пространства HSV в формат RGB. В другом частном примере осуществления способа этап f) осуществляется с помощью перевода значений ячеек матрицы в пиксели в цветовом пространстве HSV. В другом частном примере осуществления способа в каждой ячейке матрицы (I_k) записывается значение яркости пикселя в цветовой схеме HSV.

В другом частном примере осуществления способа в подматрице (I_r) вычисляют среднее арифметическое значение всех ячеек матрицы.

В другом частном примере осуществления способа осуществляют уменьшение зернистости в подматрице (I_r).

В другом частном примере осуществления способа выполняют перевод подматрицы (I_r) в монохромное полутоновое изображение.

В другом частном примере осуществления способа, на этапе b) кортеж комплексных чисел K(I*) формируется с помощью преобразования, обеспечивающего перевод рациональных значений в комплексные значения, при этом преобразование выбирается из группы: прямое/обратное преобразование Фурье, прямое/обратное дискретное быстрое преобразование Фурье (ДБПФ), косинусное преобразование, преобразование Адамара (Уолша-Адамара), преобразование Френеля. Заявленное решение также осуществляется с помощью компьютерной системы, которая содержит процессор и память, в которой хранятся машиночитаемые инструкции, выполняемые процессором для осуществления вышеуказанных способов формирования стеганографированного изображения и его дешифровки.

Описание чертежей

Фиг. 1 иллюстрирует блок-схему способа стеганографирования изображения. Фиг. 2А-2Г иллюстрируют пример внедрения цифровой метки в изображение. Фиг. 3 иллюстрирует блок-схему способа дешифрования цифровых изображений с цифровой меткой. Фиг. 4 иллюстрирует пример вычислительной системы.

Осуществление изобретения

На фиг. 1 представлена последовательность этапов, выполняемая вычислительным устройство для осуществления заявленного способа (100) стеганографирования цифрового изображения с помощью графической ЦМ. Описание способа также будет разъяснено с учетом фиг. 2А-2Д.

На первом этапе (101) вычислительная система получает входное изображение (201), в которое необходимо внедрение ЦМ. Изображение может поступать в любом пригодном цифровом формате, например, JPG, JPEG, PNG, BMP, SVG и т.п. Изображение (201) также может поступать в той или иной цветовой схеме, например, RGB, CMYK и т.п. Для полученного изображения (201) на этапе (102) создается хеш-сумма изображения, после чего осуществляется ее шифрование и создание контрольной суммы на основании зашифрованной хеш-суммы изображения. Формирование хеш-суммы может осуществляться с помощью перевода входного изображения (201) в массив байт, по которым с помощью одного из алгоритмов формируется хеш-сумма, например, алгоритмов MD2/4/5/6, SHA, SHA224, SHA256, SHA384, SHA512, ГОСТ 34.11-94 и др. Полученная хеш-сумма шифруется на приватном ключе/сертификате с применением ассиметричных криптографических алгоритмов. После шифрования хеш-суммы изображения (201) на ее основе составляется контрольная сумма, например, с применением алгоритма CRC32, или любого другого алгоритма, применяемого для аналогичных целей.

Далее на этапе (103) осуществляется формирование кортежа данных путем соединения зашифрованной хеш-суммы с контрольным значением, полученным на этапе выше.

На этапе (104) выполняется создание ЦМ (202) на основании полученного кортежа данных. ЦМ

(202) представляется в виде монохромного изображения, из которого попиксельные значения яркости образовывали кортеж данных меньшей, чем опорное изображение размерности.

Размер цифрового изображения ЦМ (202) для нанесения на входное изображение (201) определяется на основании размера шрифта, используемого при подготовке кортежа данных. Обычно, размер ЦМ не превышает 1/8 размера входного цифрового изображения (201).

На фиг. 2Б показан принцип создания монохромного изображения (203), который будет наноситься на исходное изображение - контейнер (201). Монохромное изображения (203) создается следующим образом: берется абсолютно чёрный холст (203). Посчитывается размер шрифта Font с помощью алгоритма. На холсте (203) определенным образом размещается ЦМ (202) в текстовом виде, причем биты, на которых она будет размещена, будут абсолютно белыми, таким образом. Оригинальный алгоритм обеспечивает формирование размера окна, удовлетворяющего требованию 1/8 размера входного, в котором должна поместиться текстовая информация. Выбирается максимальный размер font, например, font = 100. И до тех пор, пока текст не поместиться полностью в заданные рамки - 1/8 размера входного изображения, осуществляется последовательное уменьшение значения font на 1. Значение font первого случая, при котором текст не будет выходить за заданные рамки и будет искомым значением font.

Затем на этапе (105) выполняется формирование матрицы (I_m) значений яркости пикселей графической ЦМ (202). При выполнении данного этапа выполняется попиксельный перевод изображения ЦМ (202) из RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей изображения ЦМ (I_m). В полученной матрице (I_m) производят округление значений, лежащих в диапазоне от 0 до 1 в большую или меньшую сторону, при котором если пиксель черный, то добавляется 0 в реальную часть ячейки матрицы, координаты которой совпадают с координатами пикселя, если же пиксель белый, то добавляется коэффициент мощности в реальную часть матрицы соответственно. Округление значений в матрице (I_m) позволяет сделать изображение полностью монохромным, в независимости от искажений, которые могут иметь место. Коэффициент мощности показывает насколько белым будут выглядеть пиксели ЦМ (202) на абсолютно четном холсте (203), где 1-абсолютно белый, 0-абсолютно черный. На этапе (106) идет формирование матрицы комплексных чисел от значений яркости пикселей входного цифрового изображения (201). Данный этап выполняется с помощью перевода входного цифрового изображения (201) из полученной цветовой схемы, например, RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей изображения (I_p), и формированием матриц значений тона (H_p) и насыщенности (S_p) пикселей изображения в цветовом пространстве HSV. Далее осуществляется формирование кортежа K(Ip) из значений яркостей пикселей путем построчного перевода из полученной матрицы значений яркостей пикселей (I_p), кортежа комплексных чисел K(I_f) с помощью применения к кортежу яркостей K(I_p) прямого дискретного быстрого преобразование Фурье (ДБПФ), и последующего формирования матрицы комплексных чисел (I_f) из кортежа комплексных чисел K(I_f) той же размерности, что и матрица значений яркостей пикселей (I_p).

На этапе (107) создается промежуточная матрицы стеганограммы (I_o). На данном этапе осуществляется сложение матриц, полученных на этапах (105) и (106), для чего выполняется сложение матрицы значений яркости пикселей графической ЦМ (I_m) и матрицы комплексных чисел от значений яркости пикселей входного цифрового изображения (I_f). В результате получается промежуточная матрицы стеганограммы (I_o). Затем на этапе (108) создается матрица яркости пикселей стеганограммы (I*). Матрица (I*) создается на основе промежуточной матрицы (I_o), полученной на этапе (107), путем перевода в кортеж данных K(I_o), выполнением над этим кортежем обратного дискретного преобразования Фурье (ДБПФ). Кортеж K(I_o) переводится в матрицу размерности (I_o), производится нахождение абсолютного значения каждой ячейки, в результате чего получаем матрицу яркости пикселей стеганограммы (I*).

На этапе (109) формируют матрицу, содержащую все три значения (H_p, S_p, I*) цветового пространства HSV, описывающую стеганографированное цифровое изображение, в котором значения ячеек из матрицы яркости пикселей стеганограммы (I*), полученной на этапе (108) объединены со значениями матриц тонов (H_p) и значений насыщенностей (S_p) входного цифрового изображения, полученных на этапе (106); на этапе (110) на основе матрицы (H_p, S_p, I*), полученной на этапе (109) воспроизводят стеганографированное цифровое изображение посредством перевода каждой ячейки упомянутой матрицы (H_p, S_p, I*) из цветового пространства HSV в цветовое пространство RGB. На фиг. 3 представлена последовательность этапов, выполняемая вычислительным устройство для осуществления заявленного способа (300) демодуляции стеганографии цифрового изображения.

На этапе (301) на вход поступает изображение со стенограммой, т.е. стегоконтейнера, созданное с помощью вышеописанного способа (100). На этапе (302) осуществляется создание матрицы комплексных чисел (I_k) стегоконтейнера. Для этого выполняется перевод полученного на этапе (301) изображения в матрицу яркостей, при котором каждый пиксель стегоконтейнера, полученный в цветовом пространстве RGB, переводится в формат HSV, и в значения ячеек матрицы (I_k) записываются значения яркости.

Далее выполняется перевод матрицы яркостей (I_k) построчно в кортеж яркостей K(I_k). Над кортежем яркостей K(I_k) выполняется прямое дискретное быстрое преобразование Фурье (ДБПФ), вследствие чего получается кортеж комплексных чисел K(I*). Зная конфигурацию матрицы (I_k) на ее основании создается матрица комплексных чисел (I*).

На этапе (303) выполняется определение области стеганограммы, где находится ЦМ, учитывая ее местоположение, заложенное при выполнении способа (100). На этапе (304) происходит перевод матрицы комплексных чисел (I_r) в монохромное изображение путем вычисления абсолютного значения каждой ячейки матрицы с последующим переводом из формата HSV в формат RGB. Причем при создании формата HSV значения тона (H) и насыщенности (S) во всех ячейках раны 0. Далее на этапе (305) происходит автоматизированное распознавание ЦМ в виде изображения, например, с помощью применения нейронных сетей. После выявления ЦМ, на этапе (306) осуществляется разделение полученной на этапе (305) метки на закодированное сообщение и контрольную сумму. На этапе (307) выполняется расчет и сверка с контрольной суммой. Берется распознанное закодированное сообщение, полученное на этапе (306), для которого рассчитывается контрольная сумма по алгоритму CRC32. Если контрольная сумма, полученная в результате текущего расчета совпадает с извлеченной контрольной суммой, полученной на этапе (306), то осуществляется переход на этап (308), иначе выполняется повторное распознавание полученных данных более корректным образом и повторяется этап (306). На этапе (308) выполняется дешифрование зашифрованного сообщения с использованием открытого сертификата и получение искомой хеш-функции оригинального изображения.

Результатом работы способа (300) является хеш функция, полученная на этапе (308). Факт ее извлечения с применением открытого ключа будет являться подтверждением того, что владельцем изображения является владелец приватного (закрытого) ключа, выполнивший способ (100).

На фиг. 4 представлен общий вид вычислительного устройства (400), пригодного для выполнения вышеописанных способов (100) и (300). Устройство (400) может представлять собой устройство пользователя (300), сервер (302) и иные непредставленные устройства, которые могут участвовать в общей информационной архитектуре заявленного решения.

В общем случае вычислительное устройство (400) содержит объединенные общей шиной информационного обмена один или несколько процессоров (401), средства памяти, такие как ОЗУ (402) и ПЗУ (403), интерфейсы ввода/вывода (404), устройства ввода/вывода (405), и устройство для сетевого взаимодействия (406).

Процессор (401) (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.

ОЗУ (402) представляет собой оперативную память и предназначено для хранения исполняемых процессором (401) машиночитаемых инструкций для выполнение необходимых операций по логической обработке данных. ОЗУ (402), как правило, содержит исполняемые инструкции операционной системы и соответствующих программных компонент (приложения, программные модули и т.п.).

ПЗУ (403) 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.

Для организации работы компонентов устройства (400) и организации работы внешних подключаемых устройств применяются различные виды интерфейсов В/В (404). 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. Для обеспечения взаимодействия пользователя с вычислительным устройством (400) применяются различные средства (405) 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.

Средство сетевого взаимодействия (406) обеспечивает передачу данных устройством (400) посредством внутренней или внешней вычислительной сети, например, Интранет, Интернет, ЛВС и т.п. В качестве одного или более средств (406) 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.

Дополнительно могут применяться также средства спутниковой навигации в составе устройства (400), например, GPS, ГЛОНАСС, BeiDou, Galileo. 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 ИЗОБРЕТЕНИЯ

1. Компьютерно-реализуемый способ стеганографирования цифрового изображения с помощью графической цифровой метки (далее - ЦМ), выполняемый с помощью по меньшей мере одного процес-

сора и содержащий этапы, на которых:

a) получают по меньшей мере одно входное изображение;

b) формируют хеш-сумму упомянутого входного изображения;

c) осуществляют шифрование полученной хеш-суммы;

d) создают контрольную сумму на основании зашифрованной хеш-суммы изображения;

e) формируют кортеж данных, состоящий из полученных хеш-суммы и контрольной суммы;

f) на основе полученного кортежа формируют ЦМ в виде цифрового изображения, содержащего данные в графическом представлении;

g) формируют матрицу значений яркости пикселей графической ЦМ путем выполнения следующих этапов:

осуществляют попиксельный перевод изображения ЦМ из RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей изображения ЦМ (I_m),

в матрице значений яркостей пикселей изображения ЦМ (I_m) производят округление значений, лежащих в диапазоне от 0 до 1 в большую или меньшую сторону;

h) формируют матрицу комплексных чисел от значений яркости пикселей входного цифрового изображения путем выполнения следующих этапов:

осуществляют попиксельный перевод входного цифрового изображения из RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей изображения (I_p), и формированием матриц значений тона (H_p) и насыщенности (S_p) пикселей изображения в цветовом пространстве HSV;

формируют кортеж $K(I_p)$ из значений яркостей пикселей путем построчного перевода из полученной матрицы значений яркостей пикселей (I_p); формируют кортеж комплексных чисел $K(I_f)$ с помощью применения к кортежу яркостей прямого дискретного быстрого преобразование Фурье (ДБПФ);

формируют матрицу комплексных чисел (I_f) из кортежа комплексных чисел $K(I_f)$ той же размерности, что и матрица значений яркостей пикселей (I_p) полученной на этапе 1);

i) создают промежуточную матрицу стеганограммы (I_o) с помощью сложения матриц, полученных на этапе h) и g), причем осуществляют сложение матрицы значений яркости пикселей графической ЦМ (I_m) и матрицы комплексных чисел от значений яркости пикселей входного цифрового изображения (I_f);

j) из промежуточной матрицы стеганограммы (I_o), полученной на этапе i), формируют матрицу яркостей пикселей стеганограммы (I*) посредством быстрого обратного дискретного преобразования Фурье (ДБПФ));

k) формируют матрицу, содержащую все три значения (H_p, S_p, I*) цветового пространства HSV, описывающую стеганографированное цифровое изображение, в котором значения ячеек из матрицы яркости пикселей стеганограммы (I*), полученной на этапе j) объединены со значениями матриц тонов (H_p) и значений насыщенностей (S_p) входного цифрового изображения, полученных на этапе h);

l) на основе матрицы, полученной на этапе k) воспроизводят стеганографированное цифровое изображение посредством перевода каждой ячейки упомянутой матрицы (H_p, S_p, I*) из цветового пространства HSV в цветовое пространство RGB.

2. Способ по п.1, характеризующийся тем, что шифрование хеша осуществляется с применением ассиметричных криптографических алгоритмов на приватном ключе.

3. Способ по п.1, характеризующийся тем, что данные, формирующие ЦМ могут быть представлены в графическом виде и/или в виде буквенно-символьной последовательности.

4. Способ по п.1, характеризующийся тем, что размер цифрового изображения ЦМ для нанесения на входное изображение определяется на основании размера шрифта, используемого при подготовке кортежа данных.

5. Способ по п.4, характеризующийся тем, что размер ЦМ не превышает 1/8 размера входного цифрового изображения.

6. Способ по п.4, характеризующийся тем, что слой является черным, а буквенно-символьный кортеж данных, несущий семантику ЦМ, наносится в белом цвете.

7. Способ по п.1, характеризующийся тем, что значения яркостей пикселей входного цифрового изображения (I) построчно переводятся в матрицу яркостей K[I] исходя из фактического размера изображения в пикселях.

8. Способ по п.1, характеризующийся тем, что хеш-сумма формируется с помощью преобразования в массив байт и применения алгоритма хеширования.

9. Способ по п.8, характеризующийся тем, что алгоритм хеширования выбирается из группы: MD2/4/5/6, SHA, SHA224, SHA256, SHA384, SHA512, ГОСТ 34.11-94.

10. Способ по п.5, характеризующийся тем, что ЦМ размещается в одном из четырех возможных квадрантов изображения, условно разделенного на четыре равных фрагмента.

11. Способ по п.1, характеризующийся тем, что на этапе g) дополнительно выполняется формирование матриц значений тона (H_m) и насыщенности (S_m).

12. Способ п.1 характеризующийся тем, что на этапе h) кортеж комплексных чисел K(I*) формируется с помощью преобразования, обеспечивающего перевод рациональных значений в комплексные зна-

чения, при этом преобразование выбирается из группы: прямое/обратное преобразование Фурье, прямое/обратное дискретное быстрое преобразование Фурье (ДБПФ), косинусное преобразование, преобразование Адамара (Уолша-Адамара), преобразование Френеля.

13. Компьютерно-реализуемый способ дешифрования цифровых изображений, стеганографированных с помощью способа по любому из пп.1-12, выполняемый с помощью процессора и содержащий этапы, на которых:

a) получают входной стегоконтейнер - цифровое изображение, в котором закодирована ЦМ;

b) формируют обработанную матрицу значений яркости стегоконтейнера (I), с помощью выполнения следующих этапов:

1) осуществляют перевод изображения входного стегоконтейнера из RGB в цветовое пространство HSV с последующим построением матрицы значений яркостей пикселей (I_k);

2) формируют кортеж $K(I_k)$ из значений яркостей пикселей путем построчного перевода из полученной матрицы значений яркостей пикселей (I_k)

3) формируют кортеж комплексных чисел K(I*) значений яркости посредством быстрого обратного дискретного преобразования Фурье (ДБПФ);

4) формируют матрицу комплексных чисел (I*) из кортежа комплексных чисел K(I*) той же размерности, что и матрица значений яркостей пикселей (I_k), полученная на шаге 1);

5) рассчитывают матрицу значений яркостей пикселей стегоконтейнера (I) с помощью вычисления абсолютных значений комплексных чисел в каждой ячейки матрицы комплексных чисел (I*), полученной на предыдущем шаге;

c) определяют в обработанной матрице значений яркостей пикселей (I) подматрицу яркостей (I_r), в которой размещена ЦМ;

d) на основании подматрицы яркостей (I_r) осуществляют считывание и распознавание фрагмента изображения, содержащего закодированную ЦМ;

e) разделяют данные ЦМ на зашифрованные данные и контрольную сумму;

f) выполняют расчет и сверку контрольной суммы от зашифрованных данных с извлеченной из цифрового изображения стегоконтейнера контрольной суммой;

g) выполняют дешифрование зашифрованной части ЦМ посредством открытого ключа.

14. Способ по п.13, характеризующийся тем, что при выполнении этапа d) в тех ячейках матрицы, в которых присутствуют значения яркости выше среднего арифметического значения яркости всей матрицы, выполняется замена данных значений на нулевые.

15. Способ по п.13, характеризующийся тем, что на этапе e) уменьшение зернистости осуществляется с помощью обнуления ячеек матрицы, у которых значения соседних ячеек близки или равны 0.

16. Способ по п.13, характеризующийся тем, что при выполнении этапа f) в цветовом пространстве HSV монохромное полутоновое изображение получается путем использования яркости пикселя (I_r) из ячейки подматрицы, а насыщенность (S) и тон (H) принимают равными нулю.

17. Способ по п.13, характеризующийся тем, что полученное монохромное полутоновое изображение переводится из пространства HSV в формат RGB.

18. Способ по п.13, характеризующийся тем, что этап f) осуществляются с помощью перевода значений ячеек матрицы в пиксели в цветовом пространстве HSV.

19. Способ по п.13, характеризующийся тем, что в каждой ячейке матрицы (I_k) записывается значение яркости пикселя в цветовой схеме HSV.

20. Способ по п.13, характеризующийся тем, что в подматрице (I_r) вычисляют среднее арифметическое значение всех ячеек матрицы.

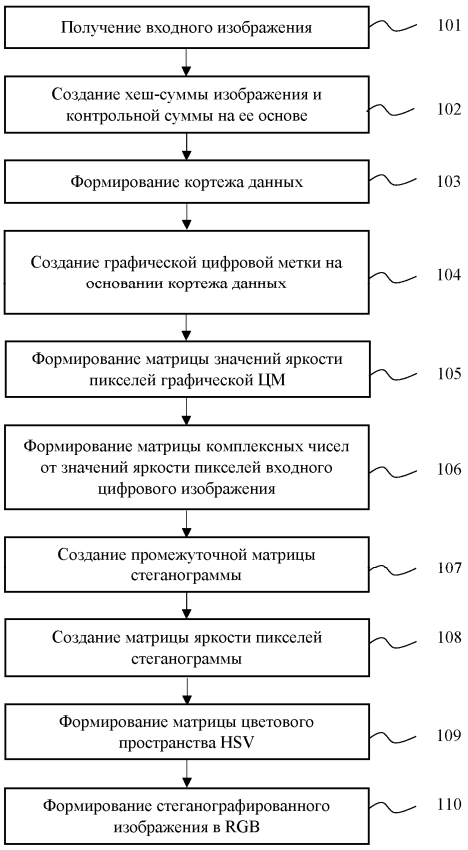
21. Способ по п.20, характеризующийся тем, что осуществляют уменьшение зернистости в подматрице (I_r).

22. Способ по п.21, характеризующийся тем, что выполняют перевод подматрицы (I_r) в монохромное полутоновое изображение.

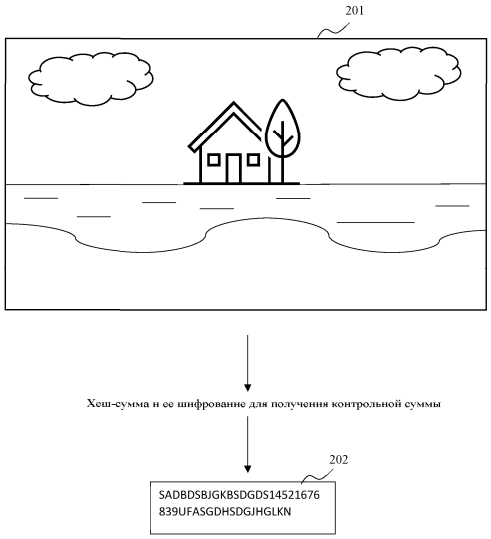
23. Способ по п.12 характеризующийся тем, что на этапе b) кортеж комплексных чисел K(I*) формируется с помощью преобразования, обеспечивающего перевод рациональных значений в комплексные значения, при этом преобразование выбирается из группы: прямое/обратное преобразование Фурье, прямое/обратное дискретное быстрое преобразование Фурье (ДБПФ), косинусное преобразование, преобразование Адамара (Уолша-Адамара), преобразование Френеля.

24. Система для стеганографирования цифрового изображения с помощью графической цифровой метки, содержащая по меньшей мере один процессор, и по меньшей мере одно средство хранения данных, содержащее машиночитаемые инструкции, которые при их выполнении процессором реализуют способ по любому из пп.1-12.

25. Система для дешифрования цифровых изображений, стеганографированных с помощью способа по любому из пп.1-12, содержащая по меньшей мере один процессор и по меньшей мере одно средство хранения данных, содержащее машиночитаемые инструкции, которые при их выполнении процессором реализуют способ по любому из пп.13-23.

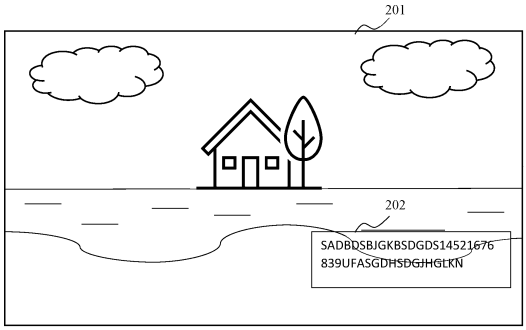


Фиг. 1

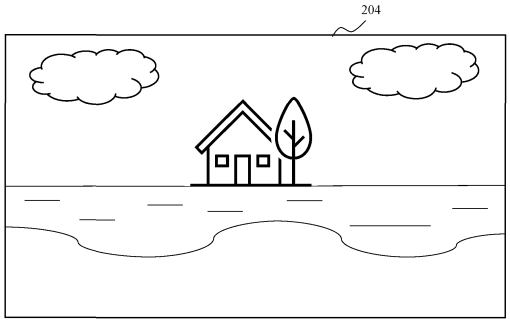


Фиг. 2А

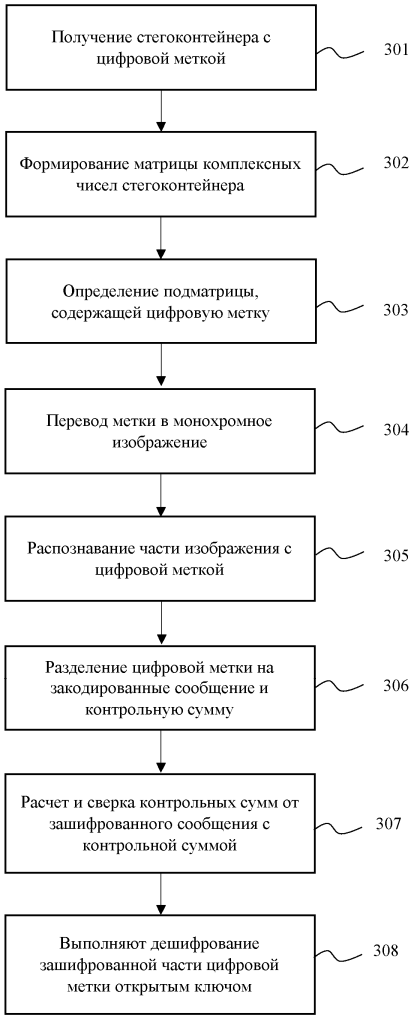
Фиг. 2Б



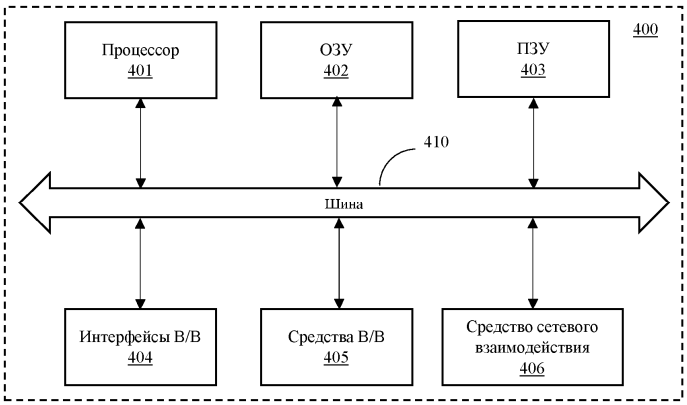
Фиг. 2В



Фиг. 2Г



Фиг. 3


Процессор
401
ОЗУ
402
ПЗУ
403
400
410
Шина
Интерфейсы В/В
404
Средства В/В
405
Средство сетевого взаимодействия
406

Фиг. 4