

(19)



**Евразийское  
патентное  
ведомство**

(11) **034104**(13) **B1**

**(12) ОПИСАНИЕ ИЗОБРЕТЕНИЯ К ЕВРАЗИЙСКОМУ ПАТЕНТУ**

**(45)** Дата публикации и выдачи патента  
**2019.12.27**

**(21)** Номер заявки  
**201800264**

**(22)** Дата подачи заявки  
**2018.04.10**

**(51)** Int. Cl. **H04N 21/835** (2011.01)  
**H04N 19/467** (2014.01)  
**G06F 21/16** (2013.01)

**(54) СПОСОБ АУТЕНТИФИКАЦИИ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, СФОРМИРОВАННЫХ С ИСПОЛЬЗОВАНИЕМ ХАОТИЧЕСКИХ ОТОБРАЖЕНИЙ**

**(43)** 2019.10.31

**(96)** 2018/ЕА/0026 (ВУ) 2018.04.10

**(71)(73)** Заявитель и патентовладелец:  
**БЕЛОРУССКИЙ  
ГОСУДАРСТВЕННЫЙ  
УНИВЕРСИТЕТ (БГУ) (ВУ)**

**(72)** Изобретатель:  
**Сидоренко Алевтина Васильевна,  
Шакинко Иван Владимирович (ВУ)**

**(56)** ГЛУМОВ Н.И. и др. Алгоритм встраивания полухрупких цифровых водяных знаков для задач аутентификации изображений и скрытой передачи информации. Компьютерная оптика, 2011, том. 35, № 2, с. 262, 264, 265

СИДОРЕНКО А.В. и др. Метод встраивания цифровых водяных знаков в изображения с использованием динамического хаоса. III Международная научно-практическая конференция "Технологии информатизации и управления", (ТИМ-2016)б, 14-15 апреля 2016 года, с. 1, 5, 6

RU-C1-2374770  
RU-C1-2636690

**(57)** Изобретение относится к вычислительной технике, а именно к методам защиты цифровых изображений при их передаче по каналам связи. Задачей изобретения является создание способа аутентификации изображений на основе цифровых водяных знаков (ЦВЗ), сформированных с использованием хаотических отображений, позволяющего обнаруживать присутствие ЦВЗ в изображении и выявлять модифицированные области изображения при наличии шума в канале связи. Решение поставленной задачи достигается тем, что способ аутентификации изображений на основе цифровых водяных знаков, сформированных с использованием хаотических отображений, включающий встраивание ЦВЗ в изображение по следующему алгоритму: получение цифрового изображения, генерация на основе исходного изображения значения параметра хаотической последовательности, формирование хаотической последовательности, представляющей собой ЦВЗ, встраивание ЦВЗ в изображение; декодирование ЦВЗ по следующему алгоритму: извлечение ЦВЗ из изображения, восстановление параметра хаотической последовательности, отличающийся тем, что в качестве восстанавливаемого параметра хаотической последовательности используют начальное значение переменной хаотического отображения, осуществляют встраивание полученной хаотической последовательности в наименьшие значащие биты значений пикселей изображения, выявляют модифицированные области изображения, осуществляя поэлементное сравнение встроенного и извлеченного ЦВЗ.

**034104 B1**

**034104 B1**

Изобретение относится к вычислительной технике, а именно к методам защиты цифровых изображений при их передаче по каналам связи.

На современном этапе развития информационных технологий широкое распространение получили изображения в цифровом виде. Передача изображений осуществляется посредством различных телекоммуникационных каналов. Поскольку не все каналы связи могут обеспечить необходимый уровень безопасности, возникает необходимость в решении задач, связанных с защитой цифровых изображений [1]. Один из подходов, использующихся для этих целей, получил название "цифровые водяные знаки". Цифровой водяной знак (ЦВЗ) - это специальная метка, встроенная в изображение (или другие цифровые данные) с тем, чтобы иметь возможность контролировать его использование [2].

Существует огромное разнообразие схем встраивания ЦВЗ в изображения [3]. При этом постоянно разрабатываются новые типы атак, направленные на ЦВЗ. Большинство данных атак ориентированы на уничтожение ЦВЗ, присутствующего в изображении. Особое место занимает атака копирования, целью которой является копирование ЦВЗ из одного изображения и добавления его к другому [4]. Это может привести к неработоспособности протоколов, использующих ЦВЗ для решения задач идентификации. Для того чтобы повысить стойкость ЦВЗ к данному типу атак, предлагается осуществлять его формирование с учетом изображения, в которое он встраивается [5]. Однако в результате помех в канале связи часть информации об исходном изображении может быть утеряна либо искажена. Это может привести к невозможности обнаружения ЦВЗ в изображении.

Известен способ формирования хрупких ЦВЗ для аутентификации изображений [6], включающий встраивание ЦВЗ в изображение по следующему алгоритму: формирование двоичной последовательности  $S$  с использованием хаотического отображения, получение ЦВЗ  $W_e$  путем поэлементного применения логической операции "исключающее или" к последовательности  $S$  и ЦВЗ  $W$ , замену значений наименьших значащих бит исходного изображения  $H$  на значения последовательности  $W_e$ ; извлечение ЦВЗ из изображения по следующему алгоритму: формирование двоичной последовательности  $S$  с использованием хаотического отображения, получение извлеченного ЦВЗ  $W_{ext}$  путем поэлементного применения логической операции "исключающее или" к последовательности  $S$  и наименьшим значащим разрядам изображения; выявление модифицированных областей изображения  $H$  путем поэлементного сравнения ЦВЗ  $W$  и  $W_{ext}$ .

Недостатком данного способа является формирование ЦВЗ без учета изображения, в которое осуществляется его встраивание, что позволяет злоумышленнику осуществлять модификацию изображения по следующему алгоритму: 1) извлечь ЦВЗ из изображения, 2) внести изменения в изображение, 3) встроить извлеченный на 1 этапе ЦВЗ в модифицированное изображение. При проведении данной атаки рассматриваемый способ окажется неспособным установить факт модификации изображения.

Известен способ формирования цифровых водяных знаков для изображений [7], включающий встраивание ЦВЗ в изображение по следующему алгоритму: 1) разделение изображения на неперекрывающиеся блоки размером  $I \times J$ , 2) модификацию выбранных бит для каждого блока, 3) вычисление хэш-значения с использованием криптографической функции, для которой входными параметрами являются пользовательский ключ, размеры изображения, модифицированный блок изображения, 4) объединение полученного хэш-значения с двоичным ЦВЗ  $B$  посредством применения операции "исключающее или", 5) добавление полученного  $S$  в изображение; извлечение ЦВЗ из изображения по следующему алгоритму: 1) модификацию выбранных бит для каждого блока изображения размером  $I \times J$ , 2) вычисление хэш-значения с использованием криптографической хэш-функции, для которой входными параметрами являются пользовательский ключ, размеры изображения, модифицированный блок изображения, 3) извлечение значений предустановленных бит из каждого блока, 4) объединение полученных значений на предыдущем шаге с вычисленными хэш-значениями посредством применения логической операции "исключающее или".

Недостатком данного способа является использование при встраивании ЦВЗ хэш-значений, вычисленных с использованием криптографической хэш-функции для блоков изображения. Это приводит к тому, что при изменении одного пикселя блока изображения, весь блок считается модифицированным. Таким образом, при наличии шумов в канале связи рассматриваемый способ не позволяет выявлять модифицированные злоумышленником блоки изображения.

Наиболее близким к предлагаемому способу является способ формирования хаотических водяных знаков для цифровых изображений [8], включающий встраивание ЦВЗ в изображение по следующему алгоритму: 1) получение цифрового изображения, 2) формирование значения параметра хаотического отображения на основе исходного изображения, 3) формирование на основе выбранного значения параметра хаотической последовательности, представляющей собой ЦВЗ, 4) встраивание ЦВЗ в изображение; декодирование ЦВЗ по следующему алгоритму: 1) извлечение ЦВЗ из изображения, 2) демодуляцию хаотической последовательности с использованием эргодического демодулятора для определения среднего значения хаотической последовательности, 3) определение значения параметра хаотического отображения.

Недостатками данного способа является использование в качестве восстанавливаемого параметра хаотической последовательности параметра хаотического отображения, что не позволяет выявлять мо-

дифицированные злоумышленником области изображения. Использование среднего значения сформированной хаотической последовательности для определения значения восстанавливаемого параметра, что делает рассматриваемый способ чувствительным к шумам в канале связи.

Задачей изобретения является создание способа аутентификации изображений на основе цифровых водяных знаков, сформированных с использованием хаотических отображений, позволяющего обнаруживать присутствие ЦВЗ в изображении и выявлять модифицированные области изображения при наличии шума в канале связи.

Решение поставленной задачи достигается тем, что в способе аутентификации изображений на основе цифровых водяных знаков, сформированных с использованием хаотических отображений, включающем встраивание ЦВЗ в изображение по следующему алгоритму: получение цифрового изображения, генерация на основе исходного изображения значения параметра хаотической последовательности, формирование хаотической последовательности, представляющей собой ЦВЗ, встраивание ЦВЗ в изображение; декодирование ЦВЗ по следующему алгоритму: извлечение ЦВЗ из изображения, восстановление параметра хаотической последовательности, отличающегося тем, что в качестве восстанавливаемого параметра хаотической последовательности используют начальное значение переменной хаотического отображения, осуществляя встраивание полученной хаотической последовательности в наименьшие значащие биты значений пикселей изображения, выявляют модифицированные области изображения, осуществляя поэлементное сравнение встроенного и извлеченного ЦВЗ.

Сущность изобретения поясняется фиг. 1-11, где

- на фиг. 1 приведена блок-схема заявляемого способа;
- на фиг. 2 - тестовое изображение "Lena.bmp" со встроенным ЦВЗ;
- на фиг. 3 - разница между исходным изображением и изображением, содержащим ЦВЗ;
- на фиг. 4 - тестовое изображение "Peppers.bmp" со встроенным ЦВЗ, сформированным для изображения "Lena.bmp";
- на фиг. 5 - результат проверки на наличие ЦВЗ в изображении "Peppers.bmp" со встроенным ЦВЗ, сформированным для изображения "Lena.bmp";
- на фиг. 6 - тестовое изображение "Lena.bmp" с добавлением шума;
- на фиг. 7 - результат проверки на наличие ЦВЗ в изображении "Lena.bmp" с добавлением шума;
- на фиг. 8 - модифицированное изображение "sailboat.bmp";
- на фиг. 9 - результаты проверки на наличие модифицированных областей для модифицированного изображения "sailboat.bmp";
- на фиг. 10 - модифицированное изображение "sailboat.bmp" с добавлением шума;
- на фиг. 11 - результат проверки на наличие модифицированных областей для модифицированного изображения "sailboat.bmp" с добавлением шума.

Блок-схема (фиг. 1) содержит модуль формирования ЦВЗ на основе хаотических отображений 1, модуль встраивания ЦВЗ в изображение 2, модуль извлечения ЦВЗ из изображения 3, модуль обратной перестановки 4, модуль восстановления начальных условий 5, модуль сравнения принятого и восстановленного ЦВЗ 6. Также на блок-схеме обозначены: 7 - начальное значение  $x_0$  для формирования ЦВЗ, 8 - значение параметра  $\lambda$  хаотического отображения, 9 - исходное изображение I, 10 - канал связи, 11 - восстановленное начальное значение  $x'_0$ .

На вход модуля 1 подаются значения параметра  $\lambda$  хаотического отображения и начальное значение  $x_0$ . Формируется последовательность значений  $y_i$ , значения элементов которой определяются согласно следующему выражению:

$$y_i = \text{floor}(x_i \cdot 256) \quad (1)$$

где  $x_i$  - значение переменной хаотического отображения на  $i$ -й итерации;

$i = 1, 2, \dots, N/8$ ;

$N$  - количество пикселей в исходном изображении I;

$\text{floor}(a)$  - наибольшее целое число, меньшее  $a$ .

После этого формируется последовательность значений  $w_k$ ,  $k = 1, 2, \dots, N$ . Элементам  $w_{8j-7}, w_{8j-6}, \dots, w_{8j}$  данной последовательности присваиваются значения разрядов числа  $y_j$ , представленного в двоичном виде. К последовательности  $w_j$  применяется процедура перестановки элементов. Перестановка может осуществляться любым способом, однако, должна быть обратимой и выглядеть как случайная.

Далее на вход модуля встраивания ЦВЗ 2 подаются изображение I и сформированная последовательность  $w_j$ . В данном модуле наименьшему значащему разряду в двоичном представлении значения  $j$ -го элемента изображения I присваивается значение  $l_j$ , которое вычисляется согласно следующему выражению:

$$l_j = W_j \oplus S[(I_j - (I_j \bmod 2))/2] \quad (2)$$

где  $\oplus$  - операция "исключающее или".

После этого изображение со встроенным ЦВЗ поступает в канал связи 10. В данном канале связи изображение может быть модифицировано вследствие шума или действий злоумышленника.

Модифицированное изображение I' поступает на вход модуля извлечения ЦВЗ 3, где происходит

вычисление значений  $w'_j$  согласно выражению (3). Штрих в данном случае указывает на то, что значения  $w'_j$  могут отличаться от значений  $w_j$  вследствие помех в канале связи

$$w'_j = I'_j \oplus [(I'_j - (I'_j \bmod 2))/2] \quad (3)$$

Последовательность значений  $w'_j$  подается на вход модуля обратной перестановки 4, где осуществляется перестановка элементов последовательности в порядке, обратном осуществляемому в модуле 1. Полученная последовательность поступает на вход модуля восстановления начального значения 5. В модуле 5 на основе значений  $w'_k$  вычисляются значения  $y_j$

$$y'_j = \sum_{z=0}^7 (2^z \cdot w'_{8j-z}) \quad (4)$$

Для восстановления начальных условий предлагается следующий оригинальный алгоритм.

1. Формирование таблицы  $T$ ,  $j$ -я строка которой содержит все возможные значения  $y_{i+1}$ , если значение  $y_i$  равно  $(j-1)$ , где  $j = 1 \text{ K } 256$ .

2. Формирование матрицы  $E$ , содержащей  $m$  строк и  $n$  столбцов,  $ij$ -й элемент матрицы  $e_{ij}$  равен единице, если представление значения  $y_i$  в двоичном виде не отличается от двоичного представления числа  $j$  не более чем в  $g$  любых разрядах. В противном случае  $e_{ij}=0$ .

3. Формирование массива пар  $B$ . Если  $e_{ij}=1$ ,  $e_{i+1,u}=1$  и в  $j$ -й строке матрицы  $T$  присутствует значение  $u$ , то пара  $(e_{ij}, e_{i+1,u})$  добавляется в массив  $B$ .

4. Выбор из пар, содержащихся в массиве  $B$ , тех, которые позволяют установить непрерывную связь между первым и последним ненулевыми элементами матрицы  $E$ . Результатом являются возможные варианты значений  $y_i$ . Стоит отметить, что при  $g = 2$  количество возможных значений для большинства элементов последовательности  $Y$  равно 1.

5. На основе  $y_n$  определяются значения  $x_{\min}$  и  $x_{\max}$  такие, что

$$x_{\min} < x_n < x_{\max} \quad (5)$$

6. Определяется значение  $x'_0$

$$x'_0 = (f^{-n}(x_{\min}) + f^{-n}(x_{\max})) / 2 \quad (6)$$

7. Вычисляются  $x'_{0,i}$

$$x'_{0,i} = x'_0 + ih \quad (7)$$

где  $h$  - положительное число;

$i = 1, \dots, M$ .

8. На основе каждого  $x'_{0,i}$  вычисляется последовательность  $y'_{i,k}$ .

Вычисляются  $d_i$ :

$$d_j = \sum_{z=1}^N (y'_{i,z} \cdot y_z) \quad (8)$$

9. В качестве  $x'_0$  выбирается такое  $x'_{0,i}$ , при использовании которого значение  $d_i$  минимально.

После этого найденное начальное значение  $x'_0$  и значение параметра  $\lambda$  поступают на вход модуля 1, где осуществляется формирование последовательности  $w''_j$ .

На вход модуля 6 поступают последовательности значений  $w'_j$  и  $w''_j$ . В данном модуле осуществляется поиск модифицированных областей изображения. Поиск модифицированных областей осуществляется следующим образом: любой блок  $D$  изображения размером  $a \times b$  пикселей, для которого отношение количества элементов  $q_b$ , значения которых различаются в фрагментах последовательностей  $w'_j$  и  $w''_j$ , соответствующих данному блоку, к общему количеству элементов блока, превосходит пороговое значение  $q_{th}$ , считается модифицированным. Пороговое значение  $q_{th}$  выбирается исходя из значения величины  $q_n$ , численно равной отношению количества модифицированных байтов на приеме к общему количеству передаваемых байтов. Рекомендуемое значение для  $q_{th}$  равно

$$q_{th} = (0.5 + q_n) / 2 \quad (9)$$

Заявляемый способ аутентификации изображений на основе цифровых водяных знаков, сформированных с использованием хаотических отображений, был реализован программно на базе персонального компьютера с установленной операционной системой "Windows 7" на языке программирования C#.

Разработанное программное обеспечение "ChaosWatermark" может работать в двух режимах: "встраивание ЦВЗ в изображение" и "проверка на наличие ЦВЗ в изображении". При помощи диалогового окна ChaosWatermark пользователь выбирает: 1) режим работы приложения, 2) изображение, в которое необходимо осуществить встраивание ЦВЗ, 3) хаотическое отображение, используемое при формировании ЦВЗ, 4) задаёт значение параметра и начальное значение выбранного хаотического отображения, 5) определяет значения параметра  $q_{th}$  и размеры блоков, используемых при поиске модифицированных областей.

Формирование ЦВЗ осуществляется посредством функции createWatermark. Данную функцию пользователь вызывает посредством щелчка мыши по кнопке "Insert Watermark" в режиме программы "встраивание ЦВЗ в изображение".

Работа функции createWatermark включает в себя следующие этапы: вызов функции initS, которая

инициализирует массив замены  $S$  и осуществляет перестановку его элементов; вызов функции  $X2Y$ , которая формирует на основе значений переменной  $x$  хаотического отображения, последовательности целых чисел и записывает их в массив  $Y$ ; вызов функции  $Y2W$ , которая преобразует полученную на предыдущем этапе последовательность целых чисел в массива бит  $W$ ; вызов функции  $permutation$ , которая осуществляет перестановку значений массива  $W$ ; вызов функции  $InsertWatermark$ , которая присваивает наименьшим значащим битам элементов изображения  $Imagel$  значения элементов массива  $W$  и записывает на диск полученное изображение  $Imagel$  в формате "bmp". После выполнения функции  $createWatermark$  пользователю отображается диалоговое окно, содержащее надпись "Complete".

Для проверки на наличие ЦВЗ в изображении и выявления модифицированных областей осуществляется вызов функции  $checkWatermark$ . Данная функция вызывается путем нажатия на кнопку "check Watermark", которая доступна только в режиме программы "Проверка на наличие ЦВЗ". При выполнении функции  $checkWatermark$  осуществляется вызов следующих вспомогательных функций:  $initS$ , которая выполняет те же операции, что и при вызове функции  $createWatermark$ ;  $extractWatermark$ , которая извлекает ЦВЗ из выбранного пользователем изображения и записывает в массив  $Wa$ ;  $inversePermutation$ , которая осуществляет обратную перестановку элементов массива  $Wa$ ;  $W2Y$  которая преобразует массив бит  $Wa$  в массив целых чисел  $Ya$ ;  $findX0$ , которая на основе массива целых чисел  $Ya$  вычисляет вещественное значение  $x_l$ ;  $X2Y$ , которая на основе значения  $x_l$  заполняет массив целых чисел  $Yb$ . Далее осуществляется вызов функции  $Y2W$ , которая на основе массива целых чисел  $Yb$  заполняет массив бит  $Wb$ . После этого осуществляется вызов функции  $permutation$ , в которую передается массив  $Wb$ . После этого в двойном цикле осуществляется обработка каждого блока изображения. Для каждого блока изображения вычисляется значение  $SM$ , равное количеству случаев, когда значения соответствующих элементов массивов  $Wb$  и  $Wa$  различаются. Если полученное значение больше величины  $q_{th}$ , то всем пикселям рассматриваемого блока изображения  $Imagel$  присваивается значение 255, что соответствует белому цвету. Осуществляется запись на диск полученного изображения  $Imagel$  в формате "bmp". В конце выполнения функции пользователю выводится сообщение "Complete" и отображается полученное изображение.

Стоит отметить что выбор изображения пользователем осуществляется посредством стандартного диалогового окна выбора файла, которое открывается по нажатию кнопки "Open image".

В качестве примера на фиг. 2-11 приводятся результаты работы предлагаемого способа для различных случаев. Пороговое значение  $q_{th}$  было выбрано равным 0,4. Результат применения предлагаемого алгоритма к тестовому изображению "Lena.bmp" представлен на фиг. 2. Поскольку процедура встраивания ЦВЗ меняет значения только наименьших значащих разрядов в двоичном представлении значений элементов изображения, визуально обнаружить присутствие ЦВЗ в изображении оказывается невозможным. Для наглядного представления отличий между исходным изображением и изображением со встроенным ЦВЗ было сформировано новое изображение  $I_s$  (фиг. 3), значения пикселей которого определялись на основе сравнения значений пикселей сравниваемых изображений. В случае, если значения пикселей в данных изображения совпадали, то соответствующему пикселю изображения  $I_s$  присваивалось значение, соответствующее черному цвету, в противном случае - значение, соответствующее белому цвету.

Для проверки стойкости предлагаемого алгоритма к атаке копирования полученный ЦВЗ для изображения "Lena.bmp" был добавлен к другим изображениям. Тестовое изображение "peppers.bmp", содержащее ЦВЗ, сформированный для изображения "Lena.bmp" представлен на фиг. 4.

На фиг. 5 представлено изображение  $I_{s2}$ , значения пикселей которого получены на основании результатов сравнения элементов последовательностей  $w'_j$  и  $w''_j$ , полученных для данного изображения.

В случае равенства значений  $w'_j$  и  $w''_j$  цвет соответствующего пикселя изображения  $I_{s2}$  выбирался черный, в противном случае - белый. Из результатов сравнения значений элементов последовательностей  $w'_j$  и  $w''_j$  установлено, что отношение  $q$  количества элементов, значения которых в данных последовательностях различаются, к общему количеству элементов в каждой последовательности превосходит значение 0,47. Поскольку полученное значение  $q$  больше значения  $q_{th}$ , делается вывод, что ЦВЗ не был обнаружен в рассматриваемом изображении.

Для оценки стойкости предлагаемого способа к наличию шума в канале связи значения выбранного количества пикселей изображения были заменены случайным образом. Изображение "Lena.bmp" при изменении значений 20% пикселей представлено на фиг. 6. Из данного изображения была извлечена последовательность  $w'_j$  и исходя из значений ее элементов определена последовательность  $w''_j$ .

На основе поэлементного сравнения значений данных последовательностей было сформировано изображение  $I_{s3}$  (фиг. 7). Количество различающихся элементов в последовательностях  $w'_j$  и  $w''_j$  составило около 25% от общего количества элементов каждой последовательности. Таким образом, для данного случая значение  $q=0,25$  примерно в полтора раза меньше порогового значения  $q_{th}$ , что свидетельствует о сохранении ЦВЗ в изображении.

При проверке предлагаемого алгоритма на способность обнаруживать модифицированные области значения размеров блоков были выбраны равными  $4 \times 4$  пикселя. Значение порогового значения  $q_{th}$  было выбрано равным 0,5. Приводятся результаты, полученные для тестового изображения "sailboat.bmp". В изображение со встроенным ЦВЗ были внесены изменения: добавлен второй парусник и дом на берегу

озера (фиг. 8). Все пиксели, принадлежащие блокам изображения, для которых  $q_B \geq q_{Bth}$ , на фиг. 9 имеют белый цвет. Таким образом, применение предлагаемого способа позволило выявить все области изображения, которые были модифицированы.

После этого была проверена способность алгоритма обнаруживать модифицированные области изображения в случае искажения значений элементов изображения вследствие наличия шума в канале связи. Для этого значения некоторых элементов изображения были изменены случайным образом. Результат работы алгоритма при изменении значений 15% элементов модифицированного изображения "sailboat.bmp", представлен на фиг. 10. Также как и в предыдущем случае, блоки изображения, для которых  $q \geq q_{th}$ , закрашены белым цветом (фиг. 11). Таким образом, в рассматриваемом случае также удалось определить те участки на изображении, которые подверглись модификации.

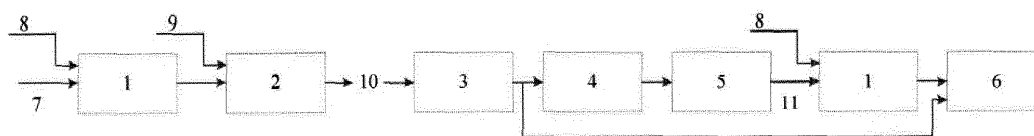
Таким образом, в сравнении с прототипом заявляемый способ аутентификации изображений на основе цифровых водяных знаков, сформированных с использованием хаотических отображений, обеспечивает более высокую степень защиты цифровых изображений от модификаций при их передаче по реальным каналам связи. При заявляемом способе оказывается возможным восстанавливать параметр хаотической последовательности при искажении отдельных ее элементов, что позволяет обнаруживать ЦВЗ в изображении и выявлять модифицированные злоумышленником области изображения при наличии шумов в канале связи.

#### Источники информации

1. Tao H. Robust Image Watermarking Theories and Techniques: A Review/H. Tao [et al.]/Journal of Applied Research and Technology. - 2014. - Vol. 12. - P. 122-138.
2. Грибунин В.Г. Цифровая стеганография/В.Г. Грибунин, И.Н. Оков, И.В. Туринцев - М.: Солон-Пресс, 2002. - С. 5.
3. Pushpa Mala S. Digital image watermarking techniques: a review/S. Pushpa Mala, D. Jayadevappa, K. Ezhilarasan//International Journal of Computer Science and Security. - 2015. - Vol. 9. - P. 140-156.
4. Kutter M. The Watermark Copy Attack/M. Kutter, S. Voloshynovskiy, A. Herrigel//Proceedings of SPIE: Security and Watermarking of Multimedia Content. San Jose, CA, USA, January 2000 - San Jose, 2000. - P. 371-380
5. Dawei Zh. A chaos-based robust wavelet-domain watermarking algorithm/Zh. Dawei, Ch. Guanrong, L. Wenbo//Chaos, solitons and fractals. - 2004. - № 22. - P. 47-54.
6. Munir R. A chaos-based fragile watermarking method in spatial domain for image authentication/International Seminar on Intelligent Technology and Its Applications. - 2015. - P. 225-22.
7. Патент US № 6504941, G06K 9/00, 2003.
8. Патент US № 2011/0142302, G06T 7/00, 2011.

#### ФОРМУЛА ИЗОБРЕТЕНИЯ

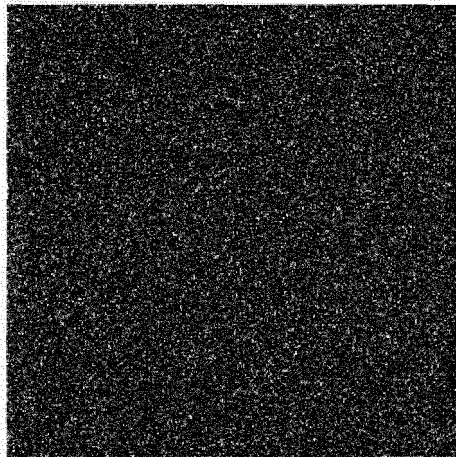
Способ аутентификации изображений на основе цифровых водяных знаков, сформированных с использованием хаотических отображений, включающий встраивание цифровых водяных знаков (ЦВЗ) в изображение по следующему алгоритму: получение цифрового изображения, генерация на основе исходного изображения значения параметра хаотической последовательности, формирование хаотической последовательности, представляющей собой ЦВЗ, встраивание ЦВЗ в изображение; декодирование ЦВЗ по следующему алгоритму: извлечение ЦВЗ из изображения, восстановление параметра хаотической последовательности, отличающийся тем, что в качестве восстанавливаемого параметра хаотической последовательности используют начальное значение переменной хаотического отображения, осуществляют встраивание полученной хаотической последовательности в наименьшие значения биты значений пикселей изображения, выявляют модифицированные области изображения, осуществляя поэлементное сравнение встроеного и извлеченного ЦВЗ.



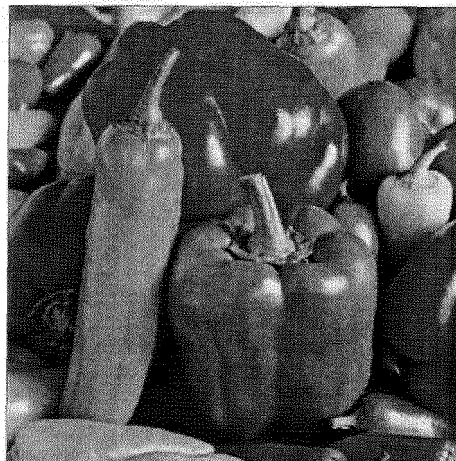
Фиг. 1



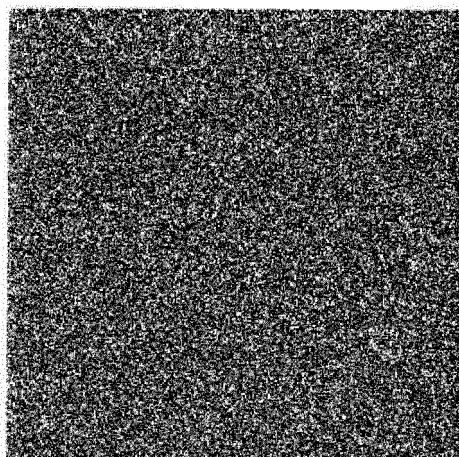
Фиг. 2



Фиг. 3



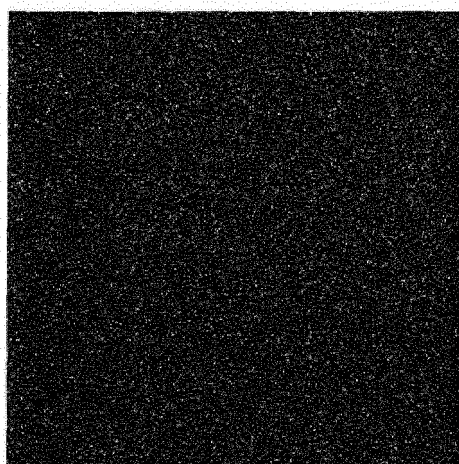
Фиг. 4



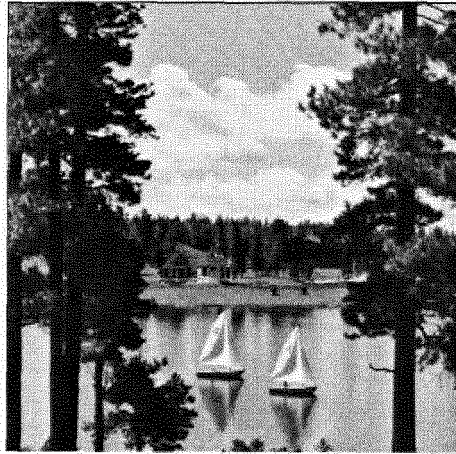
Фиг. 5



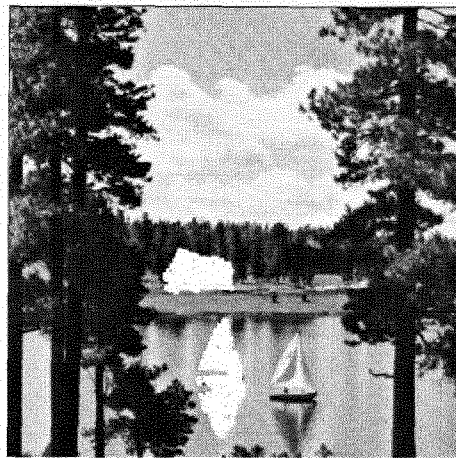
Фиг. 6



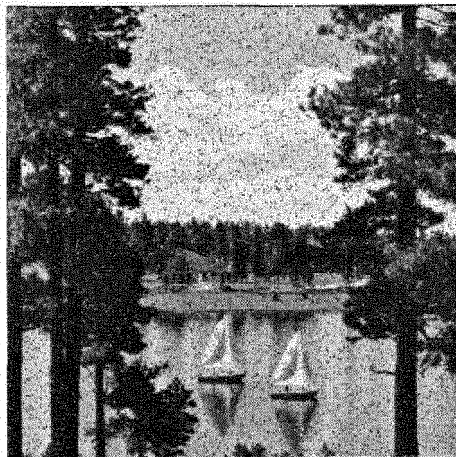
Фиг. 7



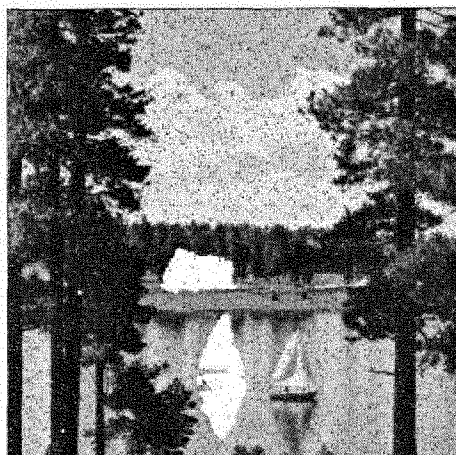
Фиг. 8



Фиг. 9



Фиг. 10



Фиг. 11

