АЛГОРИТМ ВСТРАИВАНИЯ ПОЛУХРУПКИХ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ ЗАДАЧ АУТЕНТИФИКАЦИИ ИЗОБРАЖЕНИЙ И СКРЫТОЙ ПЕРЕДАЧИ ИНФОРМАЦИИ

Глумов Н.И., Митекин В.А.
Учреждение Российской академии наук Институт систем обработки изображений РАН

Аннотация

Предложен новый алгоритм встраивания полухрупких (устойчивых к ограниченному набору искажений изображения-контейнера) цифровых водяных знаков, позволяющий одновременно решать задачи аутентификации изображения-контейнера и скрытой передачи информации. Предложенный алгоритм обладает рядом важных на практике преимуществ по сравнению с существующими алгоритмами данного класса.

Ключевые слова: цифровой водяной знак, стеганография, стегоанализ, аутентификация изображений.

Введение

Задача встраивания так называемых «хрупких» цифровых водяных знаков (далее ЦВЗ) в цифровые изображения в настоящее время имеет две наиболее актуальных сферы применения – скрытая передача информации [1] и защита цифровых изображений от модификации и подделки (аутентификация изображений) [1, 2]. В обоих случаях ключевыми являются следующие требования к встраиваемым ЦВЗ – минимизация искажений, вносимых в изображение при встраивании ЦВЗ, в особенности визуально видимых искажений, а также невозможность обнаружения и извлечения ЦВЗ без знания ключа, использованного при встраивании.

Существующие в настоящее время методы встраивания «хрупких» ЦВЗ являются узкоспециализированными и применяются либо только для скрытой передачи информации, либо только для аутентификации изображений.

В настоящей работе представлен алгоритм встраивания хрупких ЦВЗ, позволяющий одновременно обеспечивать скрытое встраивание произвольной информационной последовательности заданного объёма и обеспечивать аутентификацию изображения, в которое встроен ЦВЗ. Кроме того, как будет показано ниже, представленный алгоритм обладает рядом важных на практике преимуществ по сравнению с существующими алгоритмами обоих классов.

1. Обзор существующих алгоритмов встраивания хрупких ЦВЗ

Рассмотрим существующие алгоритмы встраивания хрупких ЦВЗ, разделив их на два класса в зависимости от выполняемых ими задач.

Алгоритмы класса 1 предназначены для защиты произвольного цифрового изображения от модификации и предполагают использование в качестве ЦВЗ либо некоторой фиксированной псевдослучайной последовательности, известной получателю [2, 3], либо последовательности, генерируемой на основе анализа изображения-контейнера (например, путём поблочного вычисления криптографической хэш-функции от изображения-контейнера [2, 4]). Далее сформированный одним из указанных выше способов ЦВЗ встраивается в изображение-контейнер таким образом, чтобы быть неустойчивым к ряду преобразований изображения-контейнера (например, масштабирование, замена фрагментов изображения-контейнера, его низко- или высокочастотная фильтрация приводят к уничтожению ЦВЗ).

Получателю изображения для того, чтобы удостовериться в его подлинности и отсутствии внесённых модификаций, необходимо извлечь из изображения ЦВЗ и сравнить его с «эталонным» ЦВЗ, который был известен получателю заранее или был вычислен как функция от полученного изображения (например, поблочная хеш-функция). Подобный способ встраивания называется схемой с полузакрытым детектором [1] и предполагает, что либо сам ЦВЗ, встроенный в изображение-контейнер, либо способ вычисления этого ЦВЗ известны и отправителю, и получателю изображения. Примеры алгоритмов данного класса представлены в [2, 4].

Алгоритмы класса 2 предназначены для встраивания в изображение произвольного ЦВЗ таким образом, чтобы сам факт встраивания не мог быть обнаружен без знания некоторой информационной последовательности фиксированной малой длины (ключа встраивания), использованной при встраивании [1-3]. В данном случае изображение со встроенным ЦВЗ выступает каналом для скрытой передачи информации (собственно, в роли передаваемой информации выступает ЦВЗ), и получатель, которому известен лишь ключ, использованный при встраивании, может обнаружить и корректно извлечь из изображения неизвестный ему ЦВЗ. Данный способ встраивания называется схемой с открытым («слепым») детектором. Примеры алгоритмов данного класса представлены в [2, 5 - 7].

Существующие алгоритмы обоих классов обладают рядом значимых недостатков. Основным недостатком алгоритмов класса 1 является неустойчивость встроенного ЦВЗ к простейшим преобразованиям изображения (линейное контрастирование, кадрирование), которые в ряде практических задач не считаются значимым искажением изображения, и, таким образом, не должны приводить к уничтожению ЦВЗ. Кроме того, использование фиксиро-

ванного ЦВЗ алгоритмами класса 1 делает возможным применение так называемой «атаки копирования ЦВЗ», позволяющей удалять встроенный ЦВЗ без знания ключа встраивания.

Одним из недостатков алгоритмов класса 2 является их непригодность для встраивания в качестве ЦВЗ непосредственно бинарных и полутоновых изображений, текста, логотипов, так как стеганографическая стойкость данных алгоритмов обеспечивается только в случае, когда ЦВЗ представляет собой некоррелированный шумоподобный сигнал. Для учёта данного ограничения большинство существующих алгоритмов используют дополнительные процедуры предобработки ЦВЗ, в том числе процедуры его шифрования, значительно повышающие вычислительную сложность алгоритмов.

В разделах 3 и 4 представлен разработанный авторами алгоритм встраивания полухрупких ЦВЗ, позволяющий одновременно выполнять задачи аутентификации изображения и скрытой передачи информации и лишённый описанных выше недостатков. Разработанный алгоритм также обеспечивает устойчивость ЦВЗ к поэлементным преобразованиям изображения-контейнера (контрастированию), кадрированию и повороту на угол, кратный 90.

2. Метод встраивания ЦВЗ на основе псевдоквантования

Предлагаемый метод встраивания основан на широко известном методе встраивания QIM с использованием модуляции яркости изображения (quantization index modulation, [3, 5, 7]). Метод встраивания QIM может быть кратко описан следующим образом. Пусть даны входное изображение $I(n, m)$ и бинарное изображение ЦВЗ $W(n, m)$, где $n \in [1, N]; m \in [1, M]$. Встраивание ЦВЗ производится следующим образом:

$$I'(n,m) = Q(I(n,m) + p(n,m), W(n,m)),$$

где $I'(n,m)$ – изображение со встроенным ЦВЗ, $p(n,m)$ – синтезированный некоррелированный шумовой сигнал, предназначенный для маскирования (dithering [5]) искажений, возникающих при переквантовании яркости исходного изображения. Знание шумового сигнала $p(n, m)$, использованного при встраивании, требуется и для извлечения ЦВЗ методом QIM, что позволяет говорить о $p(n, m)$ как о стеганографическом ключе в рамках данного метода. Функция $Q(I(n,m) + p(n,m), W(n,m))$ определяет отображение множества значений яркости пикселя изображения $I(n,m)$ на ближайшее значение из множества $\{0, q, 2 \cdot q, 3 \cdot q ...\}$ при $W(n,m) = 0$ и из множества $\{\frac{1}{2} \cdot q, \frac{3}{2} q, \frac{5}{2} q, ...\}$ при $W(n,m) = 1$ (где q – шаг квантования).

Предлагаемый в статье алгоритм, будучи основан на схожем принципе, предполагает встраивание ЦВЗ для целочисленных $I(n,m)$ и $I'(n,m)$ по следующему правилу:

$$I'(n,m) = \begin{cases} \left[\frac{I(n,m)}{q}\right] + \left\{\frac{I(n,m)}{q/2}\right\}, \\ \quad если\ W(m,n) = 0, \\ \left[\frac{I(n,m)}{q}\right] + \frac{q}{2} + \left\{\frac{I(n,m)}{q/2}\right\}, \\ \quad если\ W(m,n) = 1, \end{cases}$$

где $[\cdot]$ – операция округления до меньшего целого, $\{\cdot\}$ – остаток от деления, q – шаг квантования, определяющий степень искажения изображения-контейнера.

В данном случае для маскирования искажений, возникших при переквантовании, вместо синтезированного шумоподобного сигнала $p(n,m)$ используется компонента исходного сигнала $\left\{\frac{I(n,m)}{q/2}\right\}$, в методе QIM отбрасываемая при переквантовании. Использование данной компоненты позволяет избежать дополнительных искажений изображения, возникающих при добавлении некоррелированного шумоподобного $p(n,m)$ в методе QIM. В то же время предлагаемый метод при использовании шумоподобного ЦВЗ с равномерным распределением позволяет сохранить гистограмму изображения-контейнера близкой к гистограмме естественного изображения (рис. 1*в*).

На рис. 1*а-в* представлены гистограммы изображения-контейнера до и после встраивания ЦВЗ предлагаемым методом.

Извлечение ЦВЗ производится следующим образом:

$$W'(n,m) \in \begin{cases} 0, \ если \left[\frac{I'(n,m)}{q}\right] < \frac{q}{2}, \\ 1, \ если \left[\frac{I'(n,m)}{q}\right] \geq \frac{q}{2}, \end{cases}$$

где $W'(n,m)$ – извлечённый ЦВЗ.

На основе данного способа модуляции яркости пикселя изображения был разработан алгоритм поблочного встраивания ЦВЗ и защиты изображения от модификаций, приведённый ниже.

3. Алгоритм поблочного встраивания ЦВЗ в изображения

Предложенный метод встраивания на основе псевдоквантования, как и метод QIM, осуществляет встраивание одного пикселя (бита) ЦВЗ в один пиксель изображения-контейнера, что позволяет максимизировать объём скрытно передаваемой информации (ЦВЗ), но делает данный метод непригодным для проверки подлинности изображения [1,2].

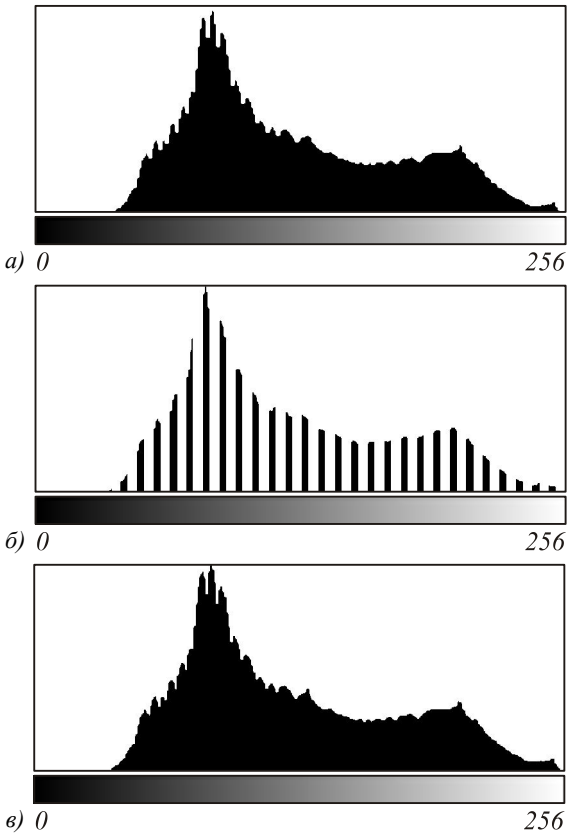


Рис. 1. Гистограммы полутонового изображения-контейнера: до встраивания ЦВЗ (а); после встраивания нулевого ЦВЗ ($W = const = 0$) (б); после встраивания ЦВЗ (в качестве ЦВЗ использован импульсный шум с вероятностью $\lambda = 0,5$) (в)

Рассмотрим алгоритм, предполагающий встраивание одного бита ЦВЗ в блок пикселей изображения-контейнера и позволяющий одновременно со скрытой передачей информации осуществлять защиту изображения-контейнера от модификации.

Пусть L – линейный размер блока пикселей изображения-контейнера, в который встраивается пиксель (бит) ЦВЗ, $K(i,j)$, где $i \in [1,L]; j \in [1,L]$ – псевдослучайное бинарное изображение-ключ (рис. 1) $W_b(u,v)$, где $u \in \left[1,\left[N/L\right]\right), v \in \left[1,\left[N/L\right]\right)$ – изображение ЦВЗ.

Тогда

$$I'(n,m) = \begin{cases} \left[\frac{I(n,m)}{q}\right] + \left\{\frac{I(n,m)}{q/2}\right\}, \\ \qquad если \hat{W}_b(n,m) = 0, \\ \left[\frac{I(n,m)}{q}\right] + q/2 + \left\{\frac{I(n,m)}{q/2}\right\}, \\ \qquad если \hat{W}_b(n,m) = 1, \end{cases}$$

где $\hat{W}_b(n,m) = \left(W_b\left[\frac{n}{L}\right], \left[\frac{m}{L}\right]\right) \oplus K\left(\left\{\frac{n}{L}\right\}, \left\{\frac{m}{L}\right\}\right)$,

$\oplus$ – операция «исключающее ИЛИ».

В случае, если значение q известно и изображение-контейнер не подвергалось никаким искажениям, извлечение бита ЦВЗ $W'(u,v)$ из блока изображения $I_b'(n,m)$, где $n \in [u \cdot L, u \cdot (L+1)], m \in [v \cdot L, v \cdot (L+1)]$, производится следующим образом:

$$W'(u,v) = \begin{cases} 0, \ если \ \forall n,m: \\ \left\{\frac{I'(n,m)}{q}\right\} - K\left(\left\{\frac{n}{L}\right\}, \left\{\frac{m}{L}\right\}\right) \cdot \frac{q}{2} < \frac{q}{2} \\ 1, \ если \ \forall n,m: \\ \left\{\frac{I'(n,m)}{q}\right\} - \bar{K}\left(\left\{\frac{n}{L}\right\}, \left\{\frac{m}{L}\right\}\right) \cdot \frac{q}{2} < \frac{q}{2} \\ \text{не определено}, \ иначе \end{cases}$$

В случае, если в результате извлечения ЦВЗ ряд значений $W'(u,v)$ не определены, подразумевается, что соответствующий блок изображения был частично или полностью модифицирован, что привело к уничтожению данного бита ЦВЗ. Фактически, вычисление $W'(u,v)$ в данном случае совмещает процедуру *извлечения ЦВЗ* (если найденный $W'(u,v)$ равен 1 или 0) и процедуру *проверки подлинности блока изображения* (т.е. обнаружения модификаций исходного изображения-контейнера – в случае, если $W'(u,v)$ не определён).

Кроме того, на практике частым является случай, когда изображение-контейнер подвергается искажениям, таким как линейное контрастирование, кадрирование и поворот, которые не изменяют содержательную составляющую изображения, но при этом делают невозможным извлечение ЦВЗ при использовании указанной выше процедуры извлечения или алгоритма QIM. Для извлечения ЦВЗ из изображений, подвергнутых указанным выше искажениям, был разработан следующий алгоритм.

В случае, когда изображение-контейнер было подвергнуто контрастированию, алгоритм *проверки подлинности блока изображения* (обнаружения ЦВЗ) имеет следующий вид.

Шаг 1. Для всех пикселей текущего блока $I_b'(n,m)$ таких, что $K\left(\{n/L\},\{m/L\}\right) = 0$, строится гистограмма яркостей $H_0(b)$.

Шаг 2. Для всех пикселей текущего блока $I_b'(n,m)$ таких, что $K\left(\{n/L\},\{m/L\}\right) = 1$, строится гистограмма яркостей $H_1(b)$.

Шаг 3. Для текущего блока вычисляется

$$D(u,v) = \begin{cases} 0, \ \sum\limits_b (H_0(b) \cdot H_1(b) = 0), \\ 1, \ \sum\limits_b (H_0(b) \cdot H_1(b) > 0). \end{cases}$$

Шаги 1-3 выполняются независимо для каждого блока изображения-контейнера $I'(n,m)$. Результатом работы алгоритма является бинарное изображе-

ние $D(u,v)$ – «карта» подлинных блоков изображения-контейнера (0 – блок подлинный и не был подвергнут искажениям после встраивания ЦВЗ, 1 – блок был подвергнут искажениям).

Аналогичным образом, путём сравнения и кластерного анализа набора гистограмм $H_0(b)$ и $H_1(b)$ вычисленного по всем блокам изображения реализуется *извлечение ЦВЗ* из изображения-контейнера, подвергнутого контрастированию.

Обеспечение устойчивости процедуры обнаружения ЦВЗ к повороту изображения-контейнера на угол, кратный 90, обеспечивается путём введения дополнительных ограничений на вид ключа $K(i,j)$, используемого при встраивании:

$$\forall i,j \in [1,\frac{L}{2}],\quad K(i,j) = K(L-j,i) =$$
$$= K(L-i,L-j) = K(j,L-i).$$

Пример псевдослучайного ключа, удовлетворяющего данным ограничениям, приведён на рис. 2.

В случае, когда было произведено кадрирование изображения-контейнера и вследствие этого произошло смещение исходных границ блоков, алгоритм *обнаружения ЦВЗ* имеет следующий вид.

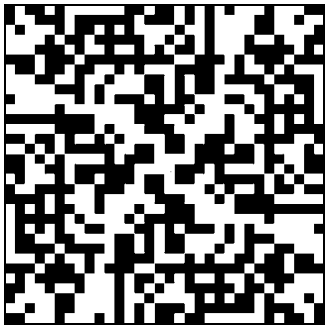


Рис. 2. Пример псевдослучайного ключа K (размер блока $L = 32$)

Шаг 1. Для всех возможных значений смещения $\Delta n, \Delta m \in [0, L-1]$ построить набор гистограмм $H_0(\Delta n, \Delta m, b)$, включающий все пиксели текущего блока $I_b^{'}(n,m)$ такие, что

$$K\left(\left\{\frac{n+\Delta n}{L}\right\},\left\{\frac{m+\Delta m}{L}\right\}\right) = 0.$$

Шаг 2. Для всех возможных значений смещения $\Delta n, \Delta m \in [0, L-1]$ построить набор гистограмм $H_1(\Delta n, \Delta m, b)$, включающий все пиксели текущего блока $I_b^{'}(n,m)$ такие, что

$$K\left(\left\{\frac{n+\Delta n}{L}\right\},\left\{\frac{m+\Delta m}{L}\right\}\right) = 1.$$

Шаг 3. Для текущего блока вычисляется «карта» подлинных блоков изображения-контейнера

$$D(u,v) =$$
$$= \begin{cases} 0, \ \min\limits_{\Delta n,\Delta m} \sum\limits_b (H_0(\Delta n,\Delta m,b)\cdot H_1(\Delta n,\Delta m,b)) = 0, \\ 1, \ \min\limits_{\Delta n,\Delta m} \sum\limits_b (H_0(\Delta n,\Delta m,b)\cdot H_1(\Delta n,\Delta m,b)) > 0. \end{cases}$$

Далее обнаружение и извлечение ЦВЗ производится аналогично предыдущему случаю.

4. Примеры работы алгоритма

В качестве иллюстрации работы предложенного алгоритма и его свойств в изображение-контейнер «Lena» размером 1024×1024 пикселей (рис. 3*а*) был встроен ЦВЗ размером 64×64 пикселя с использованием псевдослучайного ключа встраивания *K* размером 16×16 пикселей (рис. 2).

Далее изображение-контейнер было последовательно подвергнуто ряду преобразований: кадрирование со смещением исходных границ блоков (рис. 3*б*), линейное контрастирование (рис. 3*в*), поворот на 90 градусов (рис. 3*г*).

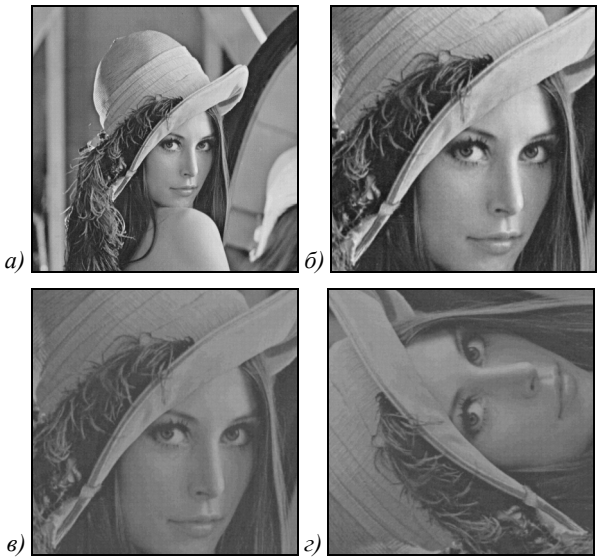
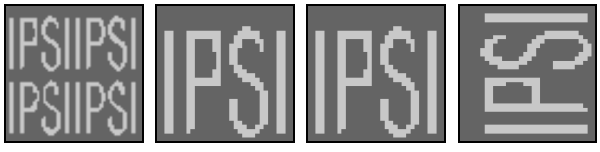


Рис. 3. Изображение-контейнер «Lena»: исходное изображение-контейнер (а), изображение после кадрирования (б), изображение после линейного контрастирования (в), изображение после поворота (г)

Из всех изображений был извлечён ЦВЗ с использованием алгоритма, представленного в разделе 3. Результаты проверки подлинности изображения и извлечения ЦВЗ, соответствующие каждому из приведённых выше изображений-контейнеров, приведены на рис. 4 *а-г*.



а) б) в) г)

Рис. 4. Результаты извлечения ЦВЗ из изображений на рис. 3 а-г

Отметим, что представленный на рис. 4*а* (отсутствие искажений изображения-контейнера) извлечённый ЦВЗ полностью идентичен исходному изображению ЦВЗ (не приведён на рисунке).

Изображение, представленное на рис. 3*г*, после встраивания ЦВЗ было последовательно подвергнуто кадрированию, контрастированию и повороту на 90 градусов. Далее в это изображение были внесены следующие модификации (рис. 5*а*):

- блок 1 изображения суммировался с гауссовским белым шумом (СКО шума $\sigma = 15$),
- блок 2 был подвергнут гауссовскому размытию (параметр расфокусировки $\sigma_p = 5$),
- блок 3b был замещён блоком 3a.

Для данного модифицированного изображения были выполнены процедуры обнаружения и извлечения ЦВЗ, результаты которых приведены на рис. 4*б-в*.

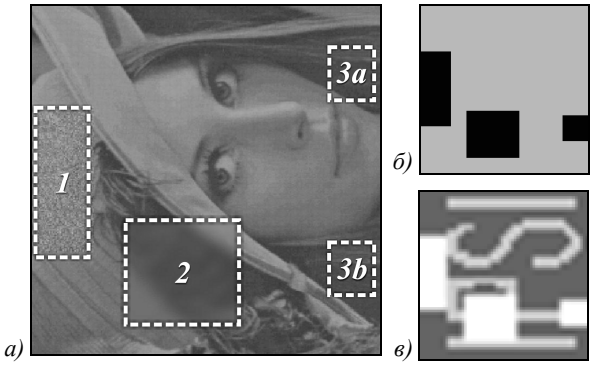


Рис. 5. Результаты обнаружения и извлечения ЦВЗ из модифицированного изображения: изображение-контейнер, представленное на рис. 3г и подвергнутое дополнительным искажениям (а); карта обнаруженных модифицированных блоков изображения-контейнера $D(u,v)$ (чёрным цветом отмечены модифицированные блоки) (б); извлечённый ЦВЗ (белым – повреждённые блоки, ЦВЗ неизвестен, тёмно-серым – 0 ЦВЗ, светло-серым – 1 ЦВЗ) (в)

Данные результаты показывают, что ЦВЗ, встроенный с использованием разработанного алгоритма, обладает устойчивостью к указанному ранее набору преобразований изображения-контейнера и даже в случае наличия подобных искажений, позволяет выявлять модифицированные области изображения. Кроме того, модификация одного или нескольких блоков изображения-контейнера приводит к потере только соответствующих бит (пикселей) ЦВЗ и не влияет на извлечение других бит.

Заключение

В работе представлен новый алгоритм поблочного встраивания ЦВЗ, обладающий следующими преимуществами по сравнению с существующими методами:

1. Алгоритм позволяет одновременно встраивать произвольный ЦВЗ в изображение-контейнер и обеспечивать проверку подлинности изображения (поблочно).

2. Алгоритм обеспечивает устойчивость ЦВЗ к преобразованиям кадрирования, линейного контрастирования и поворота на угол, кратный 90 градусам.

3. Алгоритм не требует использования дополнительных процедур предобработки (в частности, шифрования) изображения ЦВЗ.

4. Алгоритм не требует использования фиксированного ЦВЗ для обнаружения модификаций, что обеспечивает стойкость ЦВЗ к так называемым «атакам с фиксированным ЦВЗ» (watermark template attack [1], преднамеренная атака осведомлённого нарушителя, позволяющая скрывать модификации изображения даже при наличии встроенного ЦВЗ).

Благодарности

Работа выполнена при поддержке ФЦП «Научные и научно-педагогические кадры инновационной России» (контракт № 02.740.11.00001) и РФФИ (гранты 09-01-00511, 07-01-96612, 10-07-90702-моб_ст).

Литература (References)

1. **Cox, I.J.** Digital watermarking and steganography / I.J. Cox, M. Miller, J. Bloom, J. Fridrich. – San Francisco: Morgan Kaufmann Publishing, 2008. – 624 p.
2. **Fridrich, J.** Methods for Tamper Detection in Digital Images / J. Fridrich // Proceedings of ACM Workshop on Multimedia and Security. – 1999. – Vol. 1 – P. 19-23.
3. **Chen, B.** Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems / B. Chen. – Cambridge: Massachusetts Institute of Technology, 2000. – 142 p.
4. **Lin, E.T.** A review of fragile image watermarks / E.T. Lin, E.J. Delp // Proceedings of ACM Workshop on Multimedia and Security. – 1999. – Vol. 1 – P. 25-29.
5. **Chen, B.** Implementations of quantization index modulation methods for digital watermarking and information embedding / B. Chen, G.W. Wornell // Journal of VLSI Signal Processing Systems for Signal, Image, and Video Technology (Special Issue on Multimedia Signal Processing). – 2001. – Vol. 27. – P. 7-33.
6. **Lu, C.S.** Multipurpose watermarking for image authentication and protection / C.S. Lu, H.Y. Liao // IEEE Trans. Image Processing. – 2001. – Vol. 10. – P. 1579-1592.
7. **Chen, B.** Quantization index modulation: A class of provably good methods for digital watermarking and information embedding / B. Chen, G.W. Wornell // IEEE Trans. Information Theory. – 2001. – Vol. 47. – P. 1423-1443.

A NEW SEMI-FRAGILE WATERMARKING ALGORITHM FOR IMAGE AUTHENTICATION AND INFORMATION HIDING

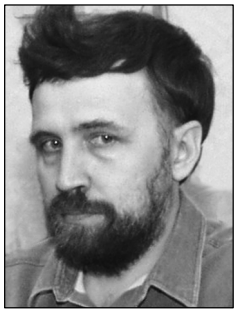
N.I. Glumov, V. A. Mitekin
Image Processing Systems Institute of Russian Academy of Sciences

Abstract

A new semi-fragile (i.e. robust to a certain set of host image modification methods) watermarking algorithm for combined data hiding and host image tampering detection is proposed, which allows to overcome several major limitations and drawbacks of an existing watermarking schemes.

Key words: digital watermarking, image authentiqation, data hiding, steganography.

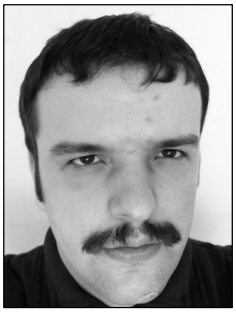
Сведения об авторах



Глумов Николай Иванович родился в 1962 году. В 1985 году окончил Куйбышевский авиационный институт (ныне Самарский государственный аэрокосмический университет имени С.П. Королёва). В 1994 году защитил диссертацию на степень кандидата технических наук. В настоящее время работает старшим научным сотрудником в Институте систем обработки изображений РАН. Круг научных интересов включает обработку изображений и распознавание образов, компрессию изображений, моделирование систем формирования цифровых изображений. Имеет свыше 100 публикаций, в том числе более 50 статей, две монографии (в соавторстве). Член Российской ассоциации распознавания образов и анализа изображений.

E-mail: *nglu@smr.ru*.

Nikolai Ivanovich Glumov (b. 1962) graduated from the Kuibyshev Aviation Institute (now Samara State Aerospace University) in 1985. In 1994 he defended his Ph.D. thesis in engineering. At present Glumov is a senior scientist at the Institute of Image Processing Systems, Russian Academy of Sciences. His scientific interests include image processing and recognition, image compression, and simulation of digital image formation systems. He has more than 100 publications, including 50 articles and two monographs (with co-authors). He is a member of the Russian Association of Image Recognition and Analysis.



Митекин Виталий Анатольевич родился в 1983 году. В 2006 году окончил Самарский государственный аэрокосмический университет имени С.П. Королёва (СГАУ) по специальности «Прикладная математика и информатика». В 2009 году защитил диссертацию на степень кандидата технических наук. В настоящее время работает научным сотрудником в Институте систем обработки изображений РАН. Круг научных интересов включает обработку изображений и распознавание образов, стеганографию и стегоанализ, криптографию. Имеет 19 публикаций, в том числе более 5 статей.

E-mail: *mitekin@smr.ru*.

Vitaly Anatolyevich Mitekin (b. 1983) graduated from the S. P. Korolyov Samara State Aerospace University (SSAU), majoring in Applied Mathematics and Informatics in 2006. He received his Candidate in Technical Sciences degree from Samara State Aerospace University in 2009. Currently he works as the researcher at the Image Processing Systems Institute of the Russian Academy of Sciences. He has 19 publications, including 5 articles. His scientific interests include image processing and recognition, steganography and steganalysis, cryptography.

Поступила в редакцию 22 февраля 2011 г.