УДК 004.932

А.А. РЕЗУНЕНКО, А.А. КОВАЛЕНКО

Полтавский военный институт связи, Украина

МЕТОД СКРЫТИЯ ИНФОРМАЦИОННЫХ СООБЩЕНИЙ В ОБЛАСТИ ПРЕОБРАЗОВАНИЯ СТАТИЧЕСКИХ ФОТОРЕАЛИСТИЧНЫХ ИЗОБРАЖЕНИЙ

Разработан метод скрытия информационных файлов в высокочастотные области вейвлет-коэффициентов статического сильнонасыщенного изображения. Показана возможность внедрения информации и в низкочастотные коэффициенты преобразования. Проведен сравнительный анализ синтезированного метода с методом внедрения информации в пространственную область изображения при пассивной атаке нарушителя. Определены показатели соответствия контейнера и стего, скрываемого и восстановленного информационного сообщения.

стеганография, контейнер, стего, вейвлет-преобразование, статическое изображение, область внедрения

Актуальность и цель исследований

Интерес к стеганографическим методам вызван несколькими важными факторами, среди которых следует отметить [1]:

– запрет криптографических методов в ряде случаев;

– необходимость защиты авторских прав на мультимедийные данные;

– изучение пиратской деятельности направленной на незаконное копирование и подделку аудиовизуальной информации и др.

В зависимости от преследуемой цели, стегоалгоритмы разделяются на стойкие (робастные), полухрупкие и хрупкие [2]. Практический интерес представляют робастные методы, к которым относится технология цифровых водяных знаков (ЦВЗ) [3]. По нашему мнению, данная технология может использовать и хрупкие методы с целью идентификации типа воздействия нарушителя на статическое изображение или невозможности его просмотра после изменения ЦВЗ.

В связи с этим, работа направлена на разработку метода внедрения информации в область преобразования изображения для исследования различных воздействий нарушителя на мультимедийные данные.

Постановка задачи на исследование

Обозначим пустой контейнер (исходное изображение) через K_C, скрываемое сообщение через I_C, а созданное стего (изображение с внедренным информационным сообщением) – K_S. Процесс выделения места скрытия сообщения состоит в следующем:

$$K_C = M_C + m_C,$$

где m_C – область скрытия данных; M_C – остаток контейнера, подвергнутого декоррелирующему преобразованию. Процесс внедрения обозначим как $\Leftrightarrow$. Тогда модифицированная область скрытия m_S равна:

$$m_S = m_C \Leftrightarrow I_C.$$

Стего образуется после обратного преобразования элементов изображения:

$$K_S = M_C + m_S.$$

Сформулируем задачу разработки стеганографического метода с учетом атаки пассивного противника (атака, направленная на выявление наличия скрытого канала передачи). Искажения, вносимые в процессе внедрения сообщения в контейнер не должны превышать допустимых:

$$K_C = M_C + m_C \equiv M_C + m_S = K_S,$$

где символ $\equiv$ означает $\varepsilon(K_C / K_S) \to \min$. Кроме

того, внедряемое сообщение I_C и извлеченное I_S должны быть идентичны, т. е.:

$$\begin{cases} PSNR\left(K_C(t)/K_S(t)\right) \geq PSNR_{\min}; \\ \sigma\left(K_C(t)/K_S(t)\right) \leq \sigma_{\max}; \\ \varepsilon\left(I_C, I_S\right) = \dfrac{\sum\limits_{i=1}^{N_1} I_C(i)\, I_S(i)}{\sum\limits_{i=1}^{N_1} I_C^2(i) \sum\limits_{i=1}^{N_1} I_S^2(i)}, \end{cases} \quad (1)$$

где N_1 – количество элементов скрываемого сообщения;

$PSNR = 10\log_{10}\left(\dfrac{255^2 \times n \times m}{\sum\limits_{i=0}^{n-1}\sum\limits_{j=0}^{m-1}\left(x_{i,j} - \tilde{x}_{i,j}\right)}\right)$ – пиковое соотношение сигнал/шум; n и m – количество строк и столбцов изображения; $x_{i,j}$ и $\tilde{x}_{i,j}$ – элементы контейнера и стего;

$\sigma = \sqrt{\dfrac{1}{n \times m}\sum\limits_{i=0}^{n-1}\sum\limits_{j=0}^{m-1}\left(x_{i,j} - \tilde{x}_{i,j}\right)^2}$ – среднеквадратическая ошибка.

В выражении (1) $PSNR_{\min} \approx 35$ дБ, $\sigma_{\max} \approx 2$ ур. квант., что соответствует граничным значениям, при которых не видны искажения стего. Данные значения *PSNR* и σ являются показателями соответствия исходного изображения восстановленному для методов сжатия изображений «почти» без потерь качества [4].

Метод скрытия информационных файлов в высокочастотные области вейвлет-коэффициентов изображения

Схематически предложенный метод внедрения информации в коэффициенты вейвлет-преобразования (ВП) представлен на рис. 1.

Метод состоит из таких основных этапов:

1. Предварительная обработка контейнера.

2. Этап внедрения информации в вейвлет-коэффициенты (ВК).

3. Формирование стего.

Предварительная обработка контейнера.

Исходное изображение формата *bmp цветовой модели RGB с параметром визуализации 24 бит/пиксель (8 бит на каждую цветовую компоненту) состоит из пикселей (далее элементов), значения которых лежит в диапазоне [0; 255]. Этап обработки контейнера заключается в ограничении диапазона представления элементов цветовых компонент. Необходимость процедуры вызвана особенностями выполнения прямого и обратного ВП.

Процедура ограничения диапазона описывается следующими выражениями:

$$\begin{cases} x_{i,j} = x_{i,j} + 2 \quad при \;\; x_{i,j} = 0 \;\; или \;\; 1; \\ x_{i,j} = x_{i,j} - 2 \quad при \;\; x_{i,j} = 254 \;\; или \;\; 255. \end{cases} \quad (2)$$

В соответствии с выражением (2) диапазон значения элементов цветовых компонент сократится и будет составлять [2; 253].

Значения элементов равные 0, 1, 254, 255 будем называть запрещенными.

Этап внедрения информации в вейвлет-коэффициенты.

Предлагается производить внедрение информации в младшие разряды высокочастотных ВК цветовых компонент контейнера. Выбор ВП как базового преобразования объясняется такими причинами:

1. Существуют целочисленные виды ВП, что позволяет избежать дополнительных искажений контейнера при формировании стего.

2. ВП позволяет разделить (декоррелировать) контейнер на низкочастотную (НЧ) и высокочастотную (ВЧ) части. Данное свойство ВП позволяет создавать робастные (внедрение сообщения в НЧ область) и хрупкие (внедрение сообщения в ВЧ область) стегоалгоритмы.

3. Выполнение декоррелирующего преобразования контейнера (необязательно ВП) делает невозможным выявление стегоканала с помощью статистического анализа передаваемых данных.

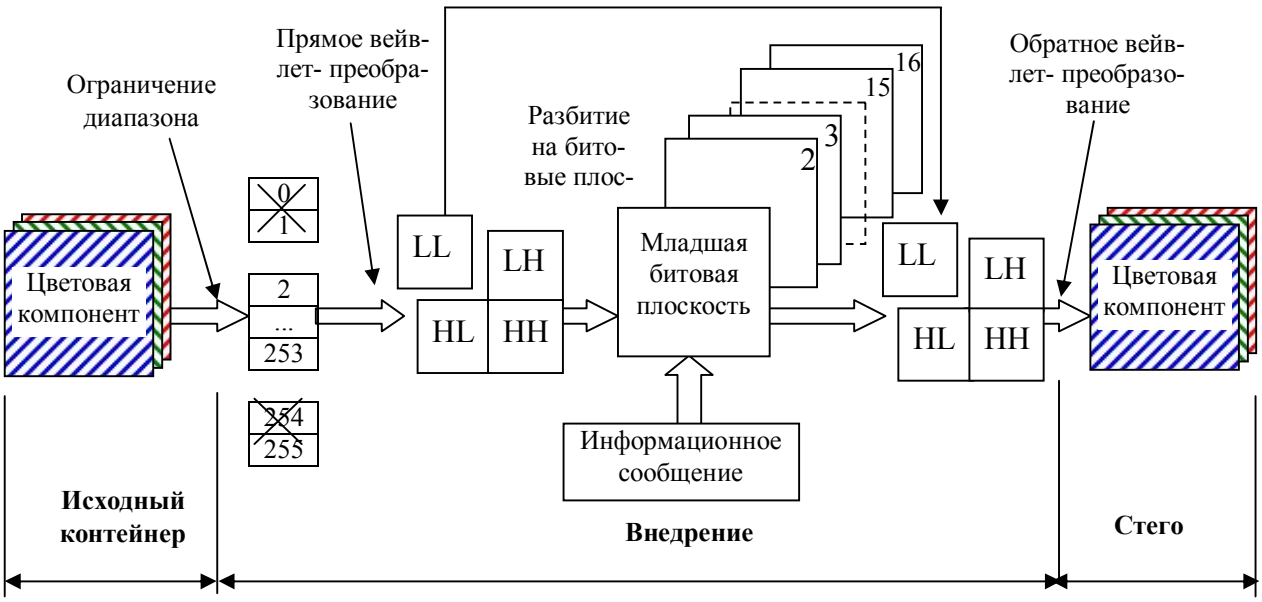


Рис. 1. Схема метода внедрения информации в область преобразования изображения

Анализ существующих видов целочисленного ВП показал, что наибольшее количество нулевых элементов в ВЧ областях (16–20%) образуется при применении к фотореалистичным сильнонасыщенным изображениям ВП Коэна-Добеши-Фово (далее ВП 5,3) [5, 6]. Поэтому целесообразно использовать его во втором этапе разработанного метода. Прямое ВП 5, 3 описывается выражениями:

$$x_n^1 = x_{2n}^0, \ \ n = 0, ..., N_1 - 1; \tag{3}$$

$$\begin{cases} H_n^1 = \left\lfloor \dfrac{x_{2n}^0 + x_{2n+2}^0}{2} \right\rfloor - x_{2n+1}^0, \ \ n = 0, ..., N_1 - 1; \\ H_{N_1-1}^1 = x_{N-2}^0 - x_{N=1}^0; \end{cases} \tag{4}$$

$$\begin{cases} L_0^1 = x_0^1 - \left\lfloor \dfrac{H_0^1}{2} \right\rfloor; \\ L_n^1 = x_n^1 - \left\lfloor \dfrac{H_{n-1}^1 + H_n^1}{4} \right\rfloor, \ \ n = 1, ..., N_1 - 1; \\ L_{N_1-1}^1 = x_{N_1-2}^1 - \left\lfloor \dfrac{H_{N_1-2}^1 + H_{N_1-1}^1}{4} \right\rfloor, \end{cases} \tag{5}$$

где H_n^1 и L_n^1 ВЧ и НЧ коэффициенты соответственно, верхний индекс означает уровень разложения, а нижний – конкретный отсчет сигнала; N – общее количество отсчетов сигнала, $N_1 = N/2$.

Процесс внедрения информации заключается в замене младшего бита ВЧ коэффициентов H_n^1 на биты сообщения I_C.

Затем выполняется обратное ВП 5,3 в соответствии с выражениями:

$$\tilde{x}_0^0 = x_0^1 + \left\lfloor \frac{H_0^1}{2} \right\rfloor; \tag{6}$$

$$\tilde{x}_{2n}^0 = x_n^1 + \left\lfloor \frac{H_{n-1}^1 + H_n^1}{4} \right\rfloor, \ \ n = 1, ..., N_1 - 1; \tag{7}$$

$$\tilde{x}_{2n+1}^0 = x_n^1 + \left\lfloor \frac{\tilde{x}_{2n}^0 + \tilde{x}_{2n+2}^1}{4} \right\rfloor - H_n^1, \ \ n = 1, ..., N_1 - 1; \tag{8}$$

$$\tilde{x}_{N-2}^0 = x_{N_1-1}^1 + \left\lfloor \frac{H_{N_1-2}^1 + H_{N_1-1}^1}{4} \right\rfloor; \tag{9}$$

$$\tilde{x}_{N-1}^0 = \tilde{x}_{N-2}^1 - H_{N_1-2}^1. \tag{10}$$

Как видно из выражений (4) и (5), в формировании одного значения коэффициента преобразования участвуют три элемента контейнера. Поэтому при использовании ВК, формировавшихся из запрещенных значений контейнера, в элементах стего после обратного ВП (выражения (6) – (10)), может возникнуть переполнение разрядной сетки. Это означает, что восстановленные после обратного ВП элементы стего, будут резко отличаться от соответст-

вующих элементов контейнера. Например, запрещенные значения «0» и «1» могут измениться на «255» и «254» и наоборот. Следовательно, изменение всего лишь отдельных элементов стего может привести к визуально заметным искажениям изображения.

Для исключения искажения элементов стего и было синтезировано аналитическое выражение (2).

Формирование стего.

Данный этап заключается в формировании выходного файла. В нем дополнительно должна быть отображена информация о наличии скрытых данных, размере внедряемого файла и его расширении. Для записи служебных данных предлагается выделить первые 32 байта полезного объема контейнера m_C. Структура служебного поля представлена на рис. 2.

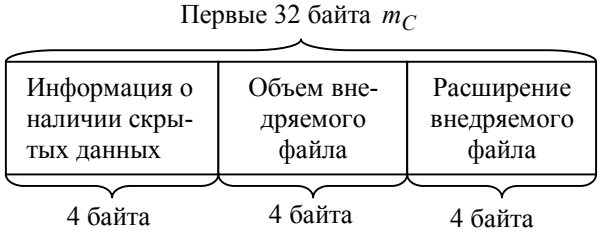


Рис. 2. Дополнительное служебное поле стего

На рис. 2 первые 4 байта задают уникальную метку о наличии скрытого файла.

Объем внедряемого файла задается 31 битом (возможность скрывать файлы объемом до 4 Гбайт), первый бит второго поля указывает на тип стеганографического метода:

– «0» – внедрение сообщения в пространственную область контейнера (декоррелирующее преобразование не используется);

– «1» – внедрение в область преобразования.

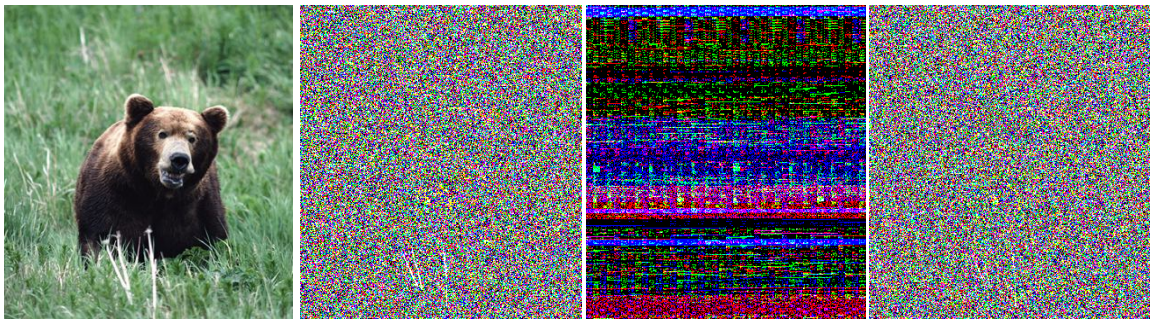
Для задания расширения необходимо 4 байта, так как стандартное расширение фалов операционной системы Windows занимает четыре символа.

Оценка разработанного метода.

Как показано в предыдущем пункте, разработанный метод предусматривает внедрение сообщения в пространственную область контейнера. В этом случае массив m_C представляет собой элементы младшей битовой плоскости контейнера. Главным недостатком такого метода является его низкая скрытность. Наличие стегоканала может выявить пассивная атака нарушителя – статистический анализ массива m_S (рис. 3).

Разработанный метод (рис. 1) устойчив к пассивной атаке, но может обладать большей стойкостью к активным воздействиям на стего, если внедрять сообщение в НЧ-область трансформант ВП (например, в LL).

Анализ рис. 3 подтверждает стойкость метода к пассивной атаке, направленной на анализ массива m_S, но не всего стего K_S.



а б в г

Рис. 3 Визуальное отображение младшей битовой плоскости (мбп) контейнера:
а – исходный контейнер; б – мбп исходного контейнера; в – мбп стего при внедрении сообщения в пространственную область; г – мбп стего при внедрении сообщения в область преобразования

Рассмотрим статистический анализ стего K_S. В этом случае о стойкости метода говорить нельзя, поскольку значения элементов контейнера K_C ограничены диапазоном [2; 253] и неизвестно как повлияет ограничение значений элементов K_C на соответствующие элементы массива K_S. Экспериментально было рассчитано количество запрещенных элементов в массиве K_C до этапа ограничения диапазона и элементов в массиве K_S (табл. 1).

Таблица 1

Процентное соотношение запрещенных элементов к общему количеству элементов в массивах K_C и K_S

Масив	Соотношение запрещенных элементов к их общему количеству, в %				
	«0»	«1»	«254»	«255»	Общее кол-во
K_C	0,315	0,023	0,038	0,845	1,22
K_S	0,011	0,061	0,131	0,013	0,216

Исследование проводилось на фотореалистичных изображениях из тестового пакета Kodak Image.

Как видно из табл. 1, число запрещенных элементов исходного контейнера и стего различно и не превышает 1,3% от общего количества элементов.

Анализ массива K_S (табл. 1) позволяет сделать несколько выводов:

1. Количество запрещенных элементов в стего меньше чем в исходном контейнере.

2. Местоположение запрещенных элементов стего изменяется по сравнению с элементами контейнера, но не более чем на три позиции по строке или столбцу (объясняется особенностями выполнения прямого и обратного ВП).

Несмотря на описанные различия в структурах стего K_S и исходного контейнера K_C, преимуществом разработанного метода является то, что запрещенные элементы снова появляются в стего, тогда как контейнер претерпел процедуру ограничения диапазона.

Изменение (но не исчезновение) местоположения запрещенных элементов в стего делает невозможным выявление стегоканала на основе статистического анализа массива K_S.

Для окончательного доказательства работоспособности разработанного метода необходимо проверить выполнения ограничений выражения (1).

Показатели объективной оценки соответствия контейнера и стего при внедрении сообщений в различное количество ВЧ областей ВП приведены на рис. 4 и 5.

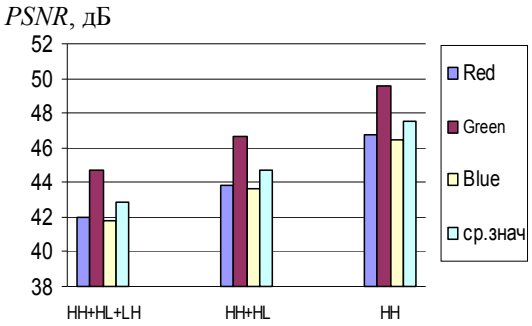


Рис. 4. Зависимость значений пикового соотношения сигнал/шум в цветовых компонентах контейнера от полезного объема контейнера

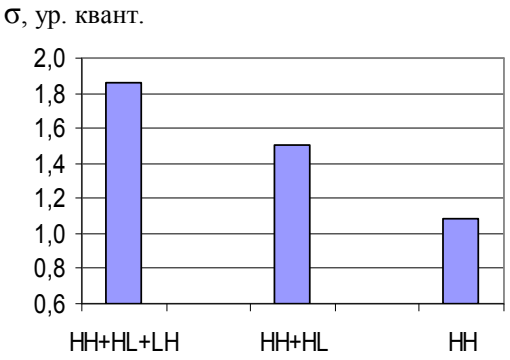


Рис. 5 Зависимость значений среднеквадратического отклонения контейнера от полезного объема контейнера

Анализ диаграмм на рис. 4 и 5 позволяет отметить:

1. Значения *PSNR* при внедрении сообщений даже во все высокочастотные области вейвлет-

преобразования не меньше 42 дБ, что удовлетворяет ограничению в формуле (1).

2. Значения σ не превышают 1,85 уровней квантования, что также удовлетворяет ограничению в (1).

Побитное сравнение файлов сообщения до внедрения и после извлечения показало, что они идентичны, т.е. $\varepsilon(I_C, I_S) = 0$.

Выводы

1. Недостатками разработанного метода по сравнению с методом внедрения сообщений в пространственную область изображения являются:

– большая вычислительная сложность;

– полезный объем контейнера уменьшается как минимум на 25% (при одноуровневом разложении изображения).

2. К преимуществам относятся:

– повышенная стойкость к пассивной атаке;

– возможность создания более стойких методов при внедрении сообщений в низкочастотную область вейвлет-преобразования.

3. Сравнение разработанного метода со стегоалгоритмом Invisible Secrets 4 показало, что значение пикового соотношения сигнал/шум выше на 3–5 дБ.

4. В дальнейшем, работа будет направлена на усовершенствование разработанного метода с целью идентификации конкретного воздействия нарушителя на статическое фотореалистичное изображение с использованием технологии цифровых водяных знаков.

Литература

1. Chun-Shie Lu. Multimedia security: steganography and digital watermarking techniques for protection of intellectual property // Institute of Information Science Academia Sinica, IGP, Hersley, London, Melbourne, Singapore, 2005. – P. 270.

2. Грибунин В. Г. Цифровая стеганография. – С.-Пб.: ВУС, 2000. – 272 с.

3. Deepa Kundur. Multiresolution Digital Watermarking: Algorithms and Implications for Multimedia, 1999. – 232 p.

4. Прэтт У.К. Цифровая обработка изображений: Кн.2. – М.: Мир, 1982. – 480 с.

5. Воробьев В. И., Грибунин В. Г. Теория и практика вейвлет-преобразования. – С.-Пб.: ВУС, 1999. – 204 с.

6. Резуненко А.А. Методы и информационная технология сжатия изображений в автоматизированных системах на основе вейвлет-преобразований: Дисс. … канд. техн. наук: 05.13.06. – Х.: НАКУ „ХАИ”, 2005. – 190 с.

Поступила в редакцию 17.01.2006

Рецензент: канд. техн. наук, доцент А.И. Тыртышников, Полтавский военный институт святи, Полтава.