УДК 004.056.53

К. В. ЗАЩЕЛКИН, А. А. ИЩЕНКО, Е. Н. ИВАНОВА

Одесский национальный политехнический университет, Украина

РЕШЕНИЕ ПРОБЛЕМЫ КЛАССИФИКАЦИИ БЛОКОВ КОНТЕЙНЕРА ПРИ JPEG-АТАКЕ НА СТЕГАНОГРАФИЧЕСКИЙ МЕТОД БЕНГАМА-МЕМОНА-ЭО-ЮНГ

Рассмотрены проблемы реализации метода Бенгама-Мемона-Эо-Юнг, выполняющего стеганографическое скрытие данных в частотную область растрового изображения. Метод позиционируется как стойкий к JPEG-сжатию изображения. Одним из важных этапов метода является классификация блоков изображения на пригодные и непригодные для встраивания информации. Показано, что в ряде случаев, JPEG-сжатие приводит к превращению пригодных блоков в непригодные. Это делает невозможным извлечение данных из изображения. В работе предлагается подход к решению данной проблемы.

Ключевые слова: *стеганография, скрытие данных, защита информации, JPEG-сжатие, дискретно-косинусное преобразование, внедрение данных, графический стего-контейнер.*

Введение

Эффективным направлением защиты информации в компьютерных системах выступают методы цифровой стеганографии. В их основе лежит принцип скрытия факта существования защищаемой информации [1]. Это принципиально отличает стенографические методы от криптографического подхода. Стеганографический подход дает возможность встраивать дополнительную скрытую информацию в стего-контейнеры, не нарушая их информационной целостности [2]. Возможные механизмы стеганографической защиты данных основаны на:

– организации скрытых каналов передачи данных внутри открытых каналов;

– скрытом хранении данных на потенциально незащищенных от несанкционированного доступа носителях информации;

– встраивании скрытых меток (цифровых водяных знаков) в различные информационные объекты с целью контроля их использования [3].

Одним из часто используемых на практике стеганографических методов является метод Бенгама-Мемона-Эо-Юнг (далее, метод БМЭЮ), выполняющий скрытие данных в частотную область растрового графического стего-контейнера [4, 5]. Данный метод отличается стойкостью к активным стего-атакам [6]. В частности, метод БМЭЮ позиционируется как стойкий к атакующим искажениям в виде JPEG-сжатия. Эта особенность метода обусловлена тем, что он, используя частотную область изображения, эффективно учитывает такие основные стадии JPEG сжатия, как разбиение изображения на блоки, дискретно-косинусное преобразование (ДКП), квантование результатов ДКП.

Метод БМЭЮ предусматривает разбиение исходного изображения-контейнера на блоки размером 8x8 пикселей и выполнение процедуры ДКП для каждого из блоков. Далее полученные результаты – блоки, представленные в области ДКП, подвергаются классификации на *пригодные* и *непригодные* для встраивания в них стего-информации. Пригодными считаются блоки, одновременно удовлетворяющие двум требованиям в пространственной области:

1) пригодные блоки не должны иметь резких перепадов яркости;

2) пригодные блоки не должны быть слишком монотонными.

Метод БМЭЮ рекомендует выполнять анализ указанных требований посредством исследования значений блоков в пространстве ДКП (рис. 1).

Рис. 1. Стандартное разбиение блока изображения в пространстве ДКП

Это исследование состоит в следующем.

1. Блоки, не отвечающие первому требованию, характеризуются наличием больших значений низкочастотных коэффициентов ДКП. Для численного разграничения того, имеют низкочастотные коэффициенты ДКП данного блока большие или малые значения вводится порог P_L. Сумма низкочастотных ДКП коэффициентов Σ_L (суммирование производится по всем низкочастотным ДКП коэффициентам блока за исключением DC-коэффициента, расположенного в левом верхнем углу блока) сравнивается с порогом P_L, в результате чего принимается решение о том, имеет ли блок резкие перепады яркости.

2. Для блоков, не отвечающих второму требованию, характерно равенство нулю большинства высокочастотных коэффициентов ДКП. Принятие решение по этому критерию производится при помощи порога P_H, с которым сравнивается сумма Σ_H высокочастотных ДКП коэффициентов блока.

Блок считается пригодным для встраивания в случае выполнения следующего составного условия:

$$(\Sigma_L < P_L) \,\&\, (\Sigma_H > P_H). \qquad (1)$$

Пороги P_L и P_H устанавливаются на стороне внедрения секретной информации в контейнер и являются частью стего-ключа, необходимого для извлечения информации.

Метод БМЭЮ предполагает, что на стороне извлечения информации из контейнера производится подсчет значений Σ_L и Σ_H и выполняется аналогичная классификация блоков на такие, в которых может содержаться встроенная стего-информация и такие, в которых такая информация содержаться не может.

1. Постановка цели работы

Проведенное исследование практической реализации метода БМЭЮ позволило выявить проблему видоизменения блоков в результате JPEG-атаки на стего-контейнер. Обнаружены случаи, при которых атака данного вида, даже при малой степени JPEG-сжатия, переводит блоки, имеющие встроенную стего-информацию (и соответственно классифицированные как пригодные) в класс непригодных для встраивания. Имеет место и обратное явление, при котором блоки, классифицированные на этапе внедрения информации, как непригодные, после сжатия могут быть отнесены к множеству пригодных и содержащих внедренную стего-информацию.

Цель данной работы состоит в усовершенствовании метода БМЭЮ путем введения в него модификации, устраняющей указанную проблему.

2. Модификация метода БМЭЮ

Предлагается модификация метода БМЭЮ, устраняющая указанную проблему и повышающая стойкость метода к стего-атакам JPEG сжатием. Модификация состоит в выполнении апостериорной классификации блоков путем применения JPEG сжатия на этапе встраивания стего-информации в контейнер. Рассмотрим предлагаемую процедуру апостериорной классификацией блоков (рис. 2).

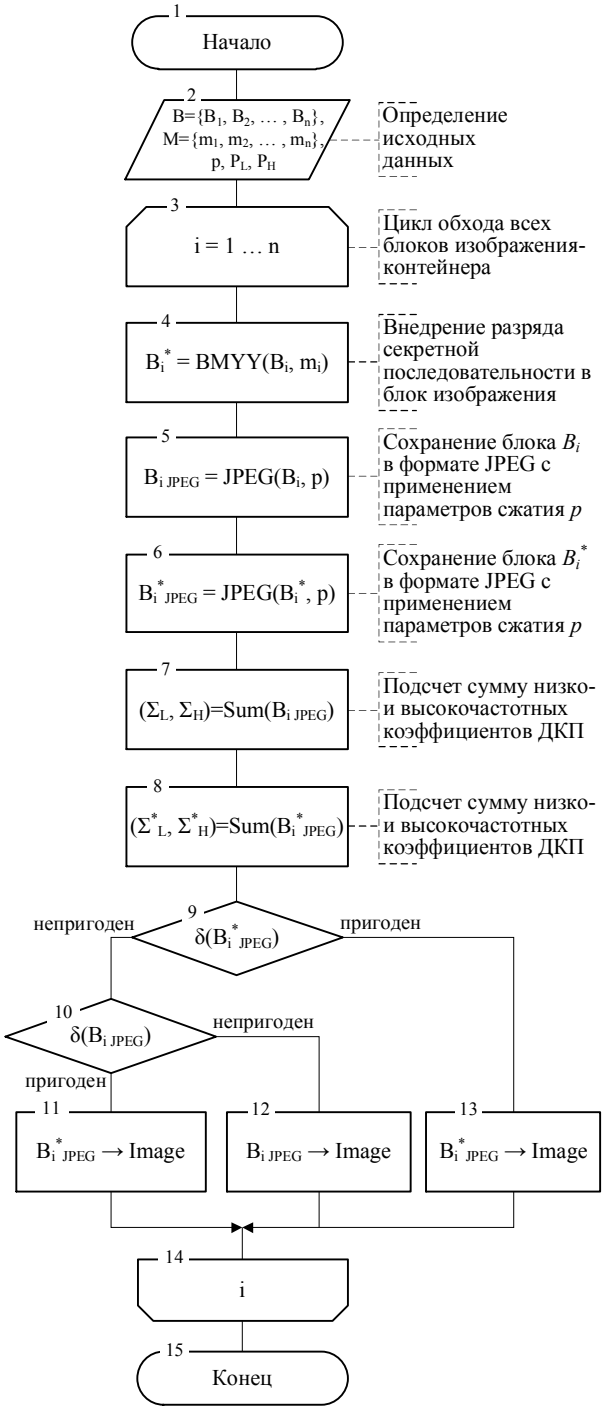

Рис. 2. Блок-схема предлагаемой апостериорной процедуры классификации блоков при встраивании

Исходные данные процедуры (рис. 2, блок 2):

– множество блоков B, на которые разбито исходное изображение-контейнер, представленных в пространстве ДКП;

– внедряемая в изображение-контейнер стего-информации, представленная двоичной последовательностью M;

– p – вектор параметров JPEG-сжатия контейнера [7], определяющий степень выраженности JPEG-атаки на заполненный стего-контейнер;

– пороги P_L и P_H, численно определяющие допустимую суммарную величину низкочастотной и высокочастотной составляющей ДКП блока.

Для определенности будем считать, что количество блоков изображения и длина внедряемой в изображение двоичной последовательности совпадают. В общем случае длина последовательности не должна превышать количество блоков.

Рассматриваемые далее действия применяются ко всем блокам изображения-контейнера и всем разрядам внедряемой в изображение последовательности (рис. 2, цикл – блок 2 и блок 14).

Шаг 1 (рис. 2, блок 4): независимо от того, относится ли текущий обрабатываемый блок B_i изображения к классу блоков, пригодных для встраивания или нет, выполняется внедрение в него в соответствии с методом БМЭЮ очередного разряда m_i двоичной последовательности M. Процедура внедрения обозначена на рис. 2 как BMYY( ). В результате такого внедрения получается модифицированный блок B_i^*.

Шаг 2 (рис. 2, блок 5): выполняется сохранение исходного блока B_i в JPEG-формат с применением параметров сжатия p. В результате получается сжатый блок $B_{i\,JPEG}$.

Шаг 3 (рис. 2, блок 6): выполняется сохранение блока B_i^*, содержащего встроенную информацию, в JPEG-формат с применением тех же параметров сжатия, что и на предыдущем шаге. В результате получается блок $B_{i\,JPEG}^*$.

Шаг 4 (рис. 2, блок 7): выполняется подсчет суммы низкочастотных и высокочастотных ДКП коэффициентов для сжатого исходного блока $B_{i\,JPEG}$.

Шаг 5 (рис. 2, блок 8): выполняется подсчет суммы низкочастотных и высокочастотных ДКП коэффициентов для сжатого блока $B_{i\,JPEG}^*$, содержащего встроенную стего-информацию.

Шаг 6 (рис. 2, блок 9): осуществляется проверка выполнения условия (1) для блока $B_{i\,JPEG}^*$. Функция проверки выполнения условия (1), обозначенная $\delta()$, возвращает значение "истина" и "ложь", выражающее выполнение или невыполнение условия. На рис. 2, значения, возвращаемые функцией $\delta()$, для наглядности, показаны как "истина" – "пригоден" и "ложь" – "непригоден", что выражает пригодность или непригодность блока для встраивания в него информации.

Если условие (рис. 2, блок 9) выполняется, то это означает, что блок $B_{i\,JPEG}^*$, содержащий встроенную стего-информацию, апостериорно признан пригодным и на стороне извлечения будет предпринята попытка извлечь информацию из этого блока.

В этом случае блок $B_{i\,JPEG}^*$ помещается в выходной стего-контейнер (рис. 2, блок 13), содержащий результат применения метода. После этого осуществляется переход к обработке следующего блока и следующего разряда встраиваемой стего-информации.

Если условие (рис. 2, блок 9) не выполняется, то осуществляется переход к следующему шагу.

Шаг 7 (рис. 2, блок 10): осуществляется проверка выполнения условия (1) для блока $B_{i\,JPEG}$. Если условие не выполняется, то это означает, что блок апостериорно признан непригодным и на стороне извлечения не будет предприниматься попытка извлечь информацию из данного блока. Это является правильным решением, так как внедренной стего-информации в блоке $B_{i\,JPEG}$ нет. В этом случае блок $B_{i\,JPEG}$ помещается в выходной стего-контейнер и осуществляется переход к обработке следующего блока и следующего разряда стего-информации.

Если условие (рис. 2, блок 10) выполняется, то это означает, что на стороне извлечения будет предпринята попытка извлечь информацию из блока $B_{i\,JPEG}$ при ее отсутствии в нем. Следовательно, в выходное изображение необходимо поместить блок, который на стороне извлечения будет признан не пригодным и не содержащим встроенной информации. В этом случае в выходное изображение помещается блок $B_{i\,JPEG}^*$ (рис. 2, блок 11), поскольку для текущей ветки блок-схемы на предыдущем шаге (рис. 2, блок 9) данный блок был признан непригодным для встраивания. Этот блок визуально не отличается от блока $B_{i\,JPEG}$, но на стороне извлечения не будет предприниматься попытка извлечь из него информацию.

После этого осуществляется переход к обработке следующего блока и следующего разряда встраиваемой стего-информации.

Предложенная процедура классификации блоков предполагает выполнение JPEG-сжатия контей-

нера на этапе внедрения информации. При этом фактически имитируется JPEG-атака на заполненный контейнер и принимается апостериорное решение о классификации блока.

3. Программная реализация и экспериментальное исследование предложенной модификации метода

Для экспериментального исследования предложенного усовершенствованного метода БМЭЮ было разработано программное обеспечение, выполняющее встраивание данных по классическому методу БМЭЮ и встраивание по методу БМЭЮ с учетом предложенной модификации.

Исходные данные эксперимента:

1) множество $\mathrm{Im} = \{\mathrm{Im}_1, \mathrm{Im}_2, \ldots, \mathrm{Im}_{100}\}$, состоящее из 100 растровых изображений, которые различающиеся:

– природой их происхождения (фотоснимки и синтетические изображения);

– размером;

– различными долями областей сплошной заливки и областей, содержащих мелкие контрастные детали;

2) множество $\mathrm{T} = \{\mathrm{T}_1, \mathrm{T}_2, \ldots, \mathrm{T}_{50}\}$, состоящее из 50 текстовых сообщений длиной от 50 до 250 символов.

Методика проведения эксперимента:

1) из множества Im случайным образом выбиралось изображение $\mathrm{im}_k \in \mathrm{Im}$;

2) из множества T случайным образом выбиралось текстовое сообщение $\mathrm{t}_q \in \mathrm{T}$;

3) сообщение t_q встраивалось в изображение im_k в соответствии с классическим вариантом метода БМЭЮ;

4) случайным образом выбирался вектор параметров JPEG-сжатия p_j, дающий степень качества сжатого изображения в диапазоне от 90 до 100 по стобалльной шкале (данный диапазон качества обычно задействован в ходе выполнения стеганографических JPEG-атак).

5) сообщение t_q встраивалось в изображение im_k в соответствии с предложенной модификацией метода БМЭЮ с применением параметра p_j для апостериорной классификации;

6) выполнялось JPEG-сжатие (стего-атака) изображений, полученных в пунктах 3 и 5. При этом применялись параметры сжатия, дающие равную или большую степень качества изображения по отношению к параметрам p_j;

7) из сжатых изображений, полученных в предыдущем пункте, в соответствии с методом БМЭЮ, извлекалась встроенная информация;

8) результаты эксперимента оценивались на основе наличия ошибок извлечения, вызванных неправильной классификацией пригодных блоков как непригодных и непригодных как пригодных.

Серия из 50 экспериментов, проведенных по указанной методике, показала, что предложенная модификация метода БМЭЮ позволяет правильно извлекать внедренные сообщения из фрагментов изображений-контейнеров, на которых традиционный метод БМЭЮ давал ошибку извлечения по причине неправильной классификации блоков, вызванной JPEG-атакой. При этом стойкость к активным стенографическим атакам, не связанным с JPEG-сжатием (незначительным размытием и поворотом изображения-контейнера) осталась неизменной по сравнению с исходным вариантом метода.

Предлагаемая модификация метода увеличивает его вычислительную сложность на этапе внедрения информации, т.к. требует дополнительных процедур JPEG-сжатия для каждого из блоков. Однако этот недостаток компенсируется устранением проблемы неверной классификации блоков на этапе извлечения информации из изображения-контейнера, подвергшегося JPEG-атаке.

Заключение

В данной работе предложено усовершенствование метода БМЭЮ, выполняющего стеганографическое внедрение данных в частотную область растрового изображения. Усовершенствование состоит в выполнении апостериорной классификации блоков изображения путем применения JPEG сжатия на этапе встраивания стего-информации в контейнер.

За счет введения предложенных модификаций были устранены ошибки извлечения, вызванные преобразованием блоков в результате JPEG-атаки на изображение-контейнер. В частности были устранены ошибки, вызванные неправильной классификацией блоков как непригодных для встраивания при их реальной пригодности и пригодных для встраивания при их реальной непригодности.

Стойкость усовершенствованного метода к активным стенографическим атакам не связанным с JPEG-сжатием при этом осталась на уровне классического метода БМЭЮ.

Литература

1. Конахович, Г.Ф. Компьютерная стеганография [Текст] / Г. Ф. Конахович, А. Ю. Пузыренко. – К. : МК-Пресс, 2006. – 288 с.

2. Fridrich, J. Steganography in Digital Media [Text] / J. Fridrich. – New York : Cambridge University Press, 2010. – 448 p.

3. Shih, F. Watermarking, Steganography, and Forensics [Text] / F. Shih. – New York : CRC Press, 2012. – 424 p.

4. Аграновский, А. В. Стеганография, цифровые водяные знаки и стегоанализ [Текст] / А. В. Аграновский, А. В. Балакин, В. Г. Грибунин. – М. : Вузовская книга, 2009. – 220 с.

5. Fast Watermarking of DCT-based Compressed Images [Text] / D. Benham, N. Memon, B. Yeo, M. Yeung. // Proc. of the International Conference on Image Science, Systems and Technology. – USA, Las Vegas – 1997. – P. 243-252.

6. Грибунин, В. Г. Цифровая стеганография [Текст] / В. Г. Грибунин. – М. : Салон-пресс, 2002. – 344 с.

7. Гонсалес, Р. Цифровая обработка изображений. [Текст] / Р. Гонсалес, Р. Вудс. – 3-е издание. – М. : Техносфера, 2012. – 1104 с.

Поступила в редакцию 20.02.2014, рассмотрена на редколлегии 25.03.2014

Рецензент: д-р техн. наук, проф. А. В. Дрозд, Одесский национальный политехнический университет, Одесса, Украина.

ВИРІШЕННЯ ПРОБЛЕМИ КЛАСИФІКАЦІЇ БЛОКІВ КОНТЕЙНЕРА ПРИ JPEG-АТАЦІ НА СТЕГАНОГРАФІЧНИЙ МЕТОД БЕНГАМА-МЕМОНА-ЕО-ЮНГ

К. В. Защолкін, А. О. Іщенко, О. М. Іванова

Розглянуто проблеми реалізації методу Бенгама-Мемона-Ео-Юнг, який виконує стеганографічне приховування даних в частотну область растрового зображення. Метод позиціонується як стійкий до JPEG-стиску зображення. Одним з важливих етапів методу є класифікація блоків зображення на придатні та непридатні для стеганографічного вбудовування. Показано, що в ряді випадків, JPEG-стиснення призводить до перетворення придатних блоків в непридатні. Це робить неможливим отримання даних з зображення. У роботі пропонується підхід до вирішення даної проблеми.

Ключові слова: стеганографія, приховування даних, захист інформації, JPEG-стиск, дискретно-косинусне перетворення, вбудовування даних, графічний стего-контейнер.

CLASSIFICATION PROBLEM SOLUTION OF CONTAINER UNITS AT JPEG-ATTACK ON STEGANOGRAPHIC METHOD OF BENHAM-MEMON-YEO-YEUNG

K. V. Zashcholkin, A. A. Ishchenko, E. N. Ivanova

Considered Benham-Memon-Yeo-Yeung method implementation problems, which performs steganography data hiding in bitmap frequency domain. The method is positioned as JPEG-image compressing resistant. One of the important stages of the method is image unit classification as usable and unusable for embedding. It is shown that in some cases, JPEG-compression results in the transformation of usable into unusable units. This makes data extraction from the image impossible. An approach to solving this problem is proposed in this paper.

Key words: steganography, data hiding, information security, JPEG-compression, discrete cosine transform, information embedding, graphics stego-container.

Защелкин Константин Вячеславович – канд. техн. наук, доцент, доцент кафедры компьютерных интеллектуальных систем и сетей, Одесский национальный политехнический университет, Одесса, Украина, e-mail: constz@te.net.ua.

Ищенко Артем Александрович – студент кафедры компьютерных интеллектуальных систем и сетей, Одесский национальный политехнический университет, Одесса, Украина.

Иванова Елена Николаевна – старший преподаватель кафедры компьютерных систем, Одесский национальный политехнический университет, Одесса, Украина.