УДК 004.056.53

РЕШЕНИЕ ПРОБЛЕМЫ КЛАССИФИКАЦИИ БЛОКОВ КОНТЕЙНЕРА ПРИ JPEG-АТАКЕ НА СТЕГОСИСТЕМУ, ПОЛУЧЕННУЮ МЕТОДОМ БЕНГАМА–МЕМОНА–ЭО–ЮНГ

К. т. н. К. В. Защелкин, А. А. Ищенко, Е. Н. Иванова

Одесский национальный политехнический университет
Украина, г. Одесса
const-z@te.net.ua

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. 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.

Эффективным направлением защиты информации в компьютерных системах являются методы цифровой стеганографии. В их основе лежит принцип скрытия факта существования защищаемой информации [1]. 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 стегоконтейнера [2]. Данный метод отличается стойкостью к активным стегоатакам [3]. 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 8×8 пикселов 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 стегоинформации. Пригодными считаются блоки, одновременно удовлетворяющие двум требованиям в пространственной области: 1) блоки не должны иметь резких перепадов яркости; 2) блоки не должны быть слишком монотонными.

Метод БМЭЮ рекомендует выполнять анализ указанных требований посредством исследования значений блоков в частотной области. А именно:

1) блоки, не отвечающие первому требованию, характеризуются наличием больших значений низкочастотных коэффициентов ДКП. Для исследования этого критерия вводится порог P_L, с которым сравнивается сумма низкочастотных ДКП-коэффициентов Σ_L (суммирование производится по всем низкочастотным ДКП-коэффициентам блока за исключением DC-коэффициента, расположенного в левом верхнем углу блока);

2) для блоков, не отвечающих второму требованию, характерно равенство нулю большинства высокочастотных коэффициентов ДКП. Для исследования этого критерия вводится порог P_H, с которым сравнивается сумма высокочастотных ДКП-коэффициентов Σ_H.

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

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

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

Проведенное исследование практической реализации метода БМЭЮ позволило выявить пробле-

му видоизменения блоков в результате JPEG-атаки на стегоконтейнер. Обнаружены случаи, при которых атака данного вида даже при малой степени сжатия переводит блоки, имеющие встроенную стегоинформацию (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 могли быть отнесены к множеству пригодных.

В настоящей работе предлагается модификация метода БМЭЮ, устраняющая указанную проблему и повышающая стойкость метода к стегоатакам JPEG-сжатием. Модификация состоит в выполнении апостериорной классификации блоков путем применения JPEG-сжатия на этапе встраивания стегоинформации в контейнер. Рассмотрим предлагаемую процедуру встраивания с апостериорной классификацией блоков. Исходные данные процедуры: очередной блок изображения B и очередной разряд m_i стегоинформации, подлежащей встраиванию.

Шаг 1. Независимо от того, относится блок B к классу пригодных для встраивания блоков или нет, внедряем в него в соответствии с методом БМЭЮ разряд m_i и получаем блок B^*.

Шаг 2. Выполняем сохранение исходного блока B в JPEG-формат с применением требуемого уровня сжатия. В результате получаем блок B_{JPEG}.

Шаг 3. Выполняем сохранение блока B^* в JPEG-формат с применением того же уровня сжатия, что и на шаге 2. В результате получаем блок B^*_{JPEG}.

Шаг 4. Проверяем, выполняется ли условие (1) для блока B^*_{JPEG}:

– если условие выполняется (это означает, что данный блок со встроенной в него стегоинформацией апостериорно признан пригодным, и на стороне извлечения будет предпринята попытка извлечь информацию из блока), то помещаем блок B^*_{JPEG} в выходной стегоконтейнер и переходим к обработке следующего блока и следующего разряда встраиваемой стегоинформации;

– если условие не выполняется, то переходим к шагу 5.

Шаг 5. Проверяем, выполняется ли условие (1) для блока B_{JPEG}:

– если условие не выполняется (это означает, что на стороне извлечения не будет предприниматься попытка извлечь информацию из блока), то помещаем блок B_{JPEG} в выходной стегоконтейнер и переходим к обработке следующего блока и следующего разряда стегоинформации;

– если условие выполняется (это означает, что на стороне извлечения будет предпринята попытка извлечь информацию из блока при ее отсутствии в нем), то помещаем блок B^*_{JPEG} (поскольку этот блок на шаге 4 признан непригодным, то на стороне извлечения не будет предприниматься попытка извлечь информацию из блока) в выходной стегоконтейнер и переходим к обработке следующего блока.

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

Проведенные эксперименты показали, что предложенная модификация метода позволяет правильно извлекать секретные сообщения из фрагментов изображений-контейнеров, на которых традиционный метод давал ошибку извлечения.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография.– Киев: МК-Пресс, 2006.– 288 с.

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

3. Грибунин В. Г. Цифровая стеганография.– Москва: Салон-пресс, 2002.– 344 с.

———————

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

Approach to the problem of classification of container units at JPEG-attacks on Benham-Memon-Yeo-Yeung steganographic system.

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

Keywords: *steganography, data hiding, information security, JPEG-compression.*