УДК 004.056.53

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА СКРЫТИЯ ДАННЫХ КУТТЕРА–ДЖОРДАНА—БОССЕНА

К. т. н. К. В. Защелкин, А. И. Иващенко, Е. Н. Иванова

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

Предлагается усовершенствование метода Куттера-Джордана-Боссена, выполняющего стеганографическое скрытие данных в пространственной области растрового изображения. Усовершенствование состоит во введении в метод дополнительных правил, устраняющих проблемы извлечения данных, характерные для некоторых случаев заполнения исходного графического контейнера.

Ключевые слова: стеганография, скрытие данных, защита информации, внедрение данных.

Стеганографические методы позволяют встраивать дополнительную информацию в цифровые объекты-контейнеры (изображения, видео, звуковые файлы), не нарушая информационной целостности последних [1]. Наиболее часто такие методы используются для защиты информации путем организации скрытых каналов передачи данных или для защиты авторских прав посредством так называемых цифровых водяных знаков [2, 3]. Одним из часто используемых стеганографических методов является метод Куттера—Джордана—Боссена (далее метод КДБ), выполняющий скрытие данных в пространственной области растровых графических стегоконтейнеров [4]. Данный метод отличается высокой стойкостью к активным стеганографическим атакам сжатием, геометрическими преобразованиями и размытием.

В рамках метода КДБ встраивание секретной двоичной последовательности $M = \{m_1, m_1, \ldots, m_n\}$ выполняется в синий канал растрового изображения-контейнера. Выбор именно синего канала обусловлен тем, что зрительная система человека наименее чувствительна к синему базовому цвету модели RGB.

Для встраивания одного бита m_i секретной последовательности в контейнере псевдослучайным образом выбирается пиксел p с координатами x и y:

$$p_{(x,y)} = \{R_{(x,y)}, G_{(x,y)}, B_{(x,y)}\}. \tag{1}$$

Для данного пиксела рассчитывается величина его яркости:

$$\lambda_{(x,y)} = 0{,}29890R_{(x,y)} + 0{,}58662G_{(x,y)} + 0{,}11448B_{(x,y)}. \tag{2}$$

После этого выполняется модификация значения синей компоненты данного пиксела согласно выражению

$$B^{new}_{(x,y)} = \begin{cases} B_{(x,y)} - \upsilon\lambda_{(x,y)} & \text{при } m_i = 0; \\ B_{(x,y)} + \upsilon\lambda_{(x,y)} & \text{при } m_i = 1, \end{cases} \tag{3}$$

где υ — константа, применяемая для всех пикселов, и определяющая энергию встраиваемого сигнала. С увеличением параметра υ растет устойчивость встроенной информации к искажениям и увеличивается «заметность» встраиваемых данных [4].

Извлечение секретной последовательности из заполненного контейнера в рамках метода КДБ производится по следующей оценке значения пиксела:

$$\widehat{B}^{*}_{(x,y)} = \frac{1}{4\sigma}\left(\sum_{i=-\sigma}^{\sigma} B^{*}_{(x+i,y)} + \sum_{j=-\sigma}^{\sigma} B^{*}_{(x,y+j)} - 2B^{*}_{(x,y)} \right), \tag{4}$$

где $\widehat{B}^{*}_{(x,y)}$ — оценочное значение синего канала пиксела с координатами (x, y);

$B^{*}_{(x+i,y)}$ и $B^{*}_{(x,y+j)}$ — значения синего канала пикселов, находящихся слева и справа, снизу и сверху от оцениваемого пиксела на расстоянии σ.

При извлечении встроенного бита вычисляется разница между текущим и оценочным значением синего канала:

$$\delta = B^*_{(x,y)} - \widehat{B}^*_{(x,y)}, \tag{5}$$

на основании которой принимается решение о значении встроенного бита по следующему правилу:

$$\begin{aligned} &\text{если } \delta < 0, \text{ то } m_i = 0; \\ &\text{если } \delta > 0, \text{ то } m_i = 1. \end{aligned} \tag{6}$$

Для уменьшения вероятности ошибки извлечения метод КДБ рекомендует встраивание каждого бита секретной последовательности производить τ раз. Секретный бит при этом извлекается по результатам усреднения разницы между реальными и оценочными значениями τ встроенных пикселов:

$$\delta = \frac{1}{\tau}\sum_{i=1}^{\tau}(B^*_{(x,y)} - \widehat{B}^*_{(x,y)}). \tag{7}$$

При практической реализации метода КДБ возникает ряд проблем, связанных с характером изображения, хранящегося в исходном стего-контейнере. Цель данной работы состоит в усовершенствовании метода КДБ путем введения в него модификаций, устраняющих указанные проблемы. Далее описываются возможные проблемы реализации метода и подходы к их устранению, в совокупности составляющие предлагаемое усовершенствование.

Проблема 1: при попытке встраивания по формуле (3) секретного бита $m_i = 1$ в область контейнера, в которой пикселы имеют максимальное значение по синему каналу, будет получено модифицированное значение, превышающее максимально возможное. В случае такого переполнения необходимо установить модифицированное значение синего канала по следующему правилу:

$$\text{если } B^{new}_{(x,y)} > 255, \text{ то } B^{new}_{(x,y)} = 255. \tag{8}$$

При этом реальное модифицированное значение фактически будет потеряно. Из-за этого при попытке извлечь секретный бит в соответствии с выражениями (4) и (5) будет получено нулевое значение переменной δ, что приведет к невозможности извлечения секретного бита по формуле (6).

Похожая проблема имеет место при попытке встраивания по формуле (3) секретного бита $m_i = 0$ в область контейнера, в которой пикселы имеют минимальное (нулевое) значение по синему каналу. В этом случае получается отрицательное модифицированное значение, что приводит к необходимости его коррекции по следующему правилу:

$$\text{если } B^{new}_{(x,y)} < 0, \text{ то } B^{new}_{(x,y)} = 0. \tag{9}$$

Потеря реального модифицированного значения здесь тоже приводит к невозможности извлечения секретного бита по формуле (6).

Игнорирование областей контейнера, содержащих максимальные или минимальные значения пикселов по синему каналу (которое снимает указанные проблемы) возможно при встраивании. Однако при извлечении распознать такие области, кроме как явным получением извлекающей стороной информации о пропускаемых пикселах, не представляется возможным.

Модификация 1: предлагается при выполнении процедуры извлечения дополнить выражение (5) следующим правилом:

$$\begin{aligned} &\text{если } (\delta = 0 \text{ и } B^*_{(x,y)} = 0), \text{ то } \delta = -0{,}5; \\ &\text{если } (\delta = 0 \text{ и } B^*_{(x,y)} = 255), \text{ то } \delta = 0{,}5. \end{aligned} \tag{10}$$

Использование правила (10) позволяет корректно извлекать встроенные значения из пикселов для которых на этапе встраивания имело место положительное или отрицательное переполнение.

Проблема 2. Данная проблема имеет место при попытке встраивания секретного бита $m_i = 1$ в область контейнера, в которой все пикселы имеют черный цвет. Если пиксел, в который производится встраивание, имеет черный цвет, т. е. все его цветовые каналы содержат нулевое значение, то яркость такого пиксела составляет $\lambda_{(x,y)} = 0$. Тогда по формуле (3) новое значение пиксела после встраивания равно $B^{new}_{(x,y)} = B_{(x,y)} + \upsilon\lambda_{(x,y)} = 0 + \upsilon \cdot 0 = 0$. При попытке извлечь секретный бит в соответствии с выражениями (4) и (5) будет получено нулевое значение переменной δ, что приведет к невозможности извлечения значения бита по формуле (6).

Модификация 2: предлагается при выполнении процедуры встраивания дополнить выражение (2) следующим правилом:

$$\text{если } \lambda = 0, \text{ то } \lambda = \alpha / \upsilon, \tag{11}$$

где $\alpha \geq 1$ — целое число, влияющее на разницу между значениями пиксела до и после встраивания. С увеличением данного параметра растет устойчивость встроенной в данный пиксел информации к искажениям и увеличивается «заметность» встраиваемых данных. Введение правила (11) позволяет корректно извлекать встроенные значения секретного бита $m_i = 1$ областей стего-контейнера, содержащих черные пикселы.

Проблема 3. Данная проблема возникает в ходе анализа значений секретного бита, τ-кратно встроенного в контейнер. В соответствии с методом КДБ, при извлечении τ раз вычисляется разница (5) между текущим и оценочным значением синего канала. В результате формируется выборка значений $\delta_i, i = 1 \ldots \tau$. Решение о значении секретного бита должно приниматься на основании усреднения (7) полученной выборки. Однако, как показывает проведенное экспериментальное исследование реализации метода КДБ, при наличии выбросов в данной выборке, может быть определено неправильно значение секретного бита. Причиной возникновения выбросов является невыполнение на некоторых фрагментах изображений предположения о том, что значение пиксела может быть установлено по значениям его соседей. Такая ситуация возникает, например, при наличии на изображении мелких деталей сильно отличающихся по цвету от их фона.

Модификация 3: предлагается перед выполнением усреднения (7), используя известные статистические методы, выявлять выбросы и исключать их из выборки либо осуществлять сглаживание выборки в месте выбросов.

Предложенные модификации метода КДБ были реализованы программно. В среде разработанного программного обеспечения были проведены экспериментальные исследования. Исходным материалом для экспериментов стали растровые изображения, различающиеся природой их происхождения (фотоснимки и синтетические изображения), размером, различными долями областей сплошной заливки и областей, содержащих мелкие контрастные детали. Проведенные эксперименты показали, что предложенные модификации метода КДБ позволяют правильно извлекать секретные сообщения из фрагментов изображений-контейнеров, на которых традиционный метод КДБ давал ошибку извлечения. За счет введения предложенных модификаций были устранены ошибки извлечения:

1) секретных битов с единичным значением из областей контейнера, в которых пикселы имеют максимальное значение по синему каналу;

2) секретных битов с нулевым значением из областей контейнера, в которых пикселы имеют минимальное (нулевое) значение по синему каналу;

3) секретных битов с единичным значением из областей контейнера, в которых все пикселы имеют черный цвет;

4) секретных битов из областей контейнера, в которых содержатся очень мелкие детали, сильно отличающихся по цвету от фона.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

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

2. Грибунин В. Г. Цифровая стеганография.— Москва: Салон-пресс, 2002.

3. Аграновский А. В., Балакин А. В., Грибунин В. Г. Стеганография, цифровые водяные знаки и стегоанализ.— Москва: Вузовская книга, 2009.

4. Kutter M., Jordan F., Bossen F. Digital Signature of Color Images using Amplitude Modulation // Proc. SPIE Storage and Retrieval for Image and Video Databases.— 1997.— Vol. 3022.— P. 518—526.

K. V. Zashcholkin, A. I. Ivaschenko, E. N. Ivanova

Improvement of the Kutter—Jordan—Bossen method of information hiding.

An improvement is proposed for the Kutter—Jordan—Bossen method performing steganography data hiding in a spatial area of a bitmap image. The improvement consists in the introduction into the method of additional rules that eliminate the problem of extracting data specific to some cases of filling the graphical container.

Keywords: *steganography, hiding data, information security, data embedding.*