УДК 004.056.53

К.В. ЗАЩЕЛКИН, А.И. ИВАЩЕНКО, Е.Н. ИВАНОВА

Одесский национальный политехнический университет

УСОВЕРШЕНСТВОВАНИЕ МЕТОДА СТЕГАНОГРАФИЧЕСКОГО СКРЫТИЯ ДАННЫХ КУТТЕРА-ДЖОРДАНА-БОССЕНА

Рассмотрена задача защиты информации путем ее стеганографического скрытия в графическом контейнере. Предлагается усовершенствование метода Куттера-Джордана-Боссена, выполняющего стеганографическое внедрение данных в пространственную область растрового изображения. Усовершенствование состоит во введении в метод дополнительных правил, устраняющих проблемы извлечения данных, характерные для некоторых случаев заполнения исходного графического контейнера. Приведены результаты исследования усовершенствованного метода в разработанной среде его программной реализации.

Ключевые слова: *стеганография, скрытие данных, защита информации, внедрение данных, графический стего-контейнер, пространственная область стего-контейнера.*

Введение

Проблема защиты информации от несанкционированного доступа является чрезвычайно актуальной на данный момент. Использование традиционных криптографических методов не снимает проблемы надежной защиты данных из-за того, что зашифрованные данные сами по себе привлекают внимание противной стороны. Результатом этого может стать применение противной стороны как методов дешифрования данных, так и «некомпьютерных» методов для получения зашифрованной информации. Исходя из этого, весьма актуальными является исследования стеганографических подходов к защите информации, которые в отличие от методов криптографии не закрывают данные от противной стороны, а скрывают от нее сам факт существования таких данных [1].

Современные стеганографические методы чаще всего основаны на встраивании секретной информации в мультимедийные контейнеры, информация в которых изначально имеет аналоговую природу: графические, звуковые, видео файлы [2]. Стеганографический подход дает возможность встраивать дополнительную информацию в стего-контейнеры не нарушая информационной целостности последних [3]. Методы стеганографии используются для защиты информации путем организации скрытых каналов передачи данных или для защиты авторских прав посредством, так называемых цифровых водяных знаков [4, 5]. Одним из часто используемых стеганографических методов является метод Куттера-Джордана-Боссена (далее метод КДБ), выполняющий скрытие данных в пространственной области растровых графических стего-контейнеров [6]. Данный метод отличается высокой стойкостью к активным стеганографическим атакам сжатием, геометрическими преобразованиями и размытием.

В рамках метода КДБ встраивание секретной двоичной последовательности $M = \{m_1, m_1, \dots, m_n\}$ 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 [7].

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

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

где $R_{(x,y)}, G_{(x,y)}, B_{(x,y)}$ – соответственно красная, зеленая и синяя цветовая компоненты пикселя.

Для данного пикселя стандартным способом рассчитывается величина его яркости [8]:

$$\lambda_{(x,y)} = 0,298R_{(x,y)} + 0,586G_{(x,y)} + 0,114B_{(x,y)}. \quad (2)$$

После этого, в соответствии со следующим выражением выполняется модификация значения синей компоненты данного пикселя:

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

где υ – константа, применяемая для всех пикселей, и определяющая энергию встраиваемого сигнала. С увеличением параметра υ растет устойчивость встроенной информации к искажениям и увеличивается «заметность» встраиваемых данных [6].

Извлечение секретной последовательности из

заполненного контейнера, в рамках метода КДБ, производится по следующей оценке значения пикселя:

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

где $\hat{B}^{*}_{(x,y)}$ – оценочное значение синего канала пикселя с координатами (x, y);

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

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

$$\delta = B^{*}_{(x,y)} - \hat{B}^{*}_{(x,y)}. \quad (5)$$

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

$$\begin{aligned} &\text{if } \delta < 0, \text{ then } m_i = 0; \\ &\text{if } \delta > 0, \text{ then } m_i = 1. \end{aligned} \quad (6)$$

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 пикселей:

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

При увеличении величины τ снижается вероятность ошибки извлечения, но, при этом, уменьшается объем данных, которые можно внедрить в контейнер.

Постановка задачи

Проведенное исследование практической реализации метода КДБ позволило выявить ряд проблем, связанных с характером изображения, хранящегося в исходном стего-контейнере. Проблемы встраивания, и соответственно извлечения, секретных данных возникают при наличии в исходном контейнере областей, в которых большинство пикселей имеют:

1) максимальное значение по синему каналу;

2) нулевое значение по синему каналу;

3) черный цвет (минимальное значение по всем цветовым каналам).

Кроме того, имеется проблема извлечения данных из контейнера по методу КДБ, связанная с наличием выбросов в выборке значений, полученных в результате анализа секретного бита τ-кратно встроенного в контейнер.

Цель данной работы состоит в усовершенствовании метода КДБ путем введения в него модификаций, устраняющих указанные проблемы.

Далее в работе описывается природа выявленных проблем реализации метода КДБ и подходы к их устранению, в совокупности, составляющие предлагаемое усовершенствование.

Модификации метода Куттера-Джордана-Боссена

Проблема 1: при попытке встраивания по формуле (3) секретного бита $m_i = 1$ в область контейнера, в которой пиксели 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:

$$\text{if } B^{new}_{(x,y)} > 255 \text{ then } B^{new}_{(x,y)} = 255. \quad (8)$$

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 пиксели имеют минимальное (нулевое) значение по синему каналу. В этом случае получается отрицательное модифицированное значение, что приводит к необходимости его коррекции по следующему правилу:

$$\text{if } B^{new}_{(x,y)} < 0 \text{ then } B^{new}_{(x,y)} = 0. \quad (9)$$

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

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

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

$$\begin{aligned} &\text{if } (\delta = 0 \text{ and } B^{*}_{(x,y)} = 0) \text{ then } \delta = -0,5; \\ &\text{if } (\delta = 0 \text{ and } B^{*}_{(x,y)} = 255) \text{ then } \delta = 0,5. \end{aligned} \quad (10)$$

Использование правила (10) позволяет корректно извлекать встроенные значения из пикселей, 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 об-

ласть контейнера, в которой все пиксели имеют черный цвет. Если пиксель, в который производится встраивание, имеет черный цвет, т.е. все его цветовые каналы содержат нулевое значение, то яркость такого пикселя составляет $\lambda_{(x,y)} = 0$. Тогда по формуле (3) новое значение пикселя 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:

$$\text{if } \lambda = 0 \text{ then } \lambda = \alpha/\upsilon, \qquad (11)$$

где $\alpha \geq 1$ – целое число, влияющее на разницу между значениями пикселя до и после встраивания. С увеличением данного параметра растет устойчивость, встроенной в данный пиксель информации к искажениям и увеличивается «заметность» встраиваемых данных. Действительно, подстановка значения λ из выражения (11) в формулу (3) приводит к прибавлению или вычитанию значения α от значения синего канала пикселя $B_{(x,y)}$. Такое изменение будет затрагивать младшие $\lfloor \log_2 \alpha \rfloor + 1$ двоичных разрядов $B_{(x,y)}$ и приводить к погрешности $\pm\alpha$.

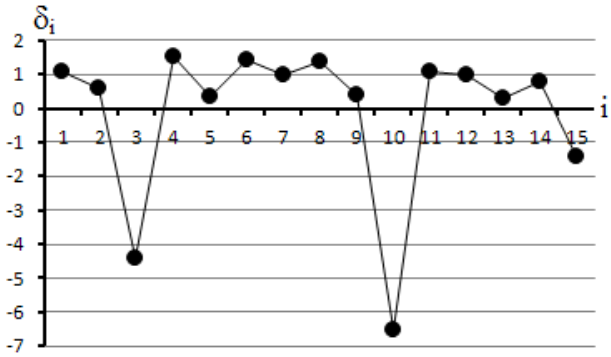
Введение правила (11) позволяет корректно извлекать встроенные значения секретного бита $m_i = 1$ из областей стего-контейнера, содержащих черные пиксели.

Проблема 3. Данная проблема возникает в ходе анализа значений секретного бита τ-кратно встроенного в контейнер. В соответствии с методом КДБ, при извлечении секретной информации τ раз вычисляется разница (5) между текущим и оценочным значением синего канала для определенным образом размещенных пикселей. 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 (рис. 1), значение секретного бита может быть определено неправильно.

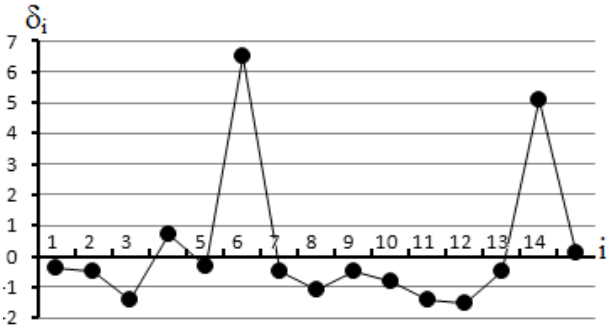
Причиной возникновения выбросов является невыполнение на некоторых фрагментах изображений предположения о том, что значение пикселя может быть установлено по значениям его соседей. Такая ситуация возникает, например, при наличии на изображении мелких деталей сильно отличающихся по цвету от их фона. Эта особенность изображения может иметь как естественную природу, так и быть следствием наличия шума типа «соль и перец» [7].

На рис. 1 а показан пример выбросов в выборке, полученной при извлечении 15-кратно встроенного секретного бита. Как видно, большинство компонентов выборки являются положительными и имеют небольшое значение. Наличие отрицательных выбросов в точках 3 и 10 приводит к неверному определению значения секретного бита по формулам (7) и (6). В данном примере вместо верного единичного значения секретного бита будет получено неверное нулевое значение.

Похожая проблема имеет место в случае положительных выбросов при отрицательных значениях большинства компонентов выборки (рис. 1 б). В данном примере наличие положительных выбросов в точках 6 и 14 приводит к тому, что вместо верного нулевого значения секретного бита, будет получено неверное единичное значение.



а



б

Рис. 1. Пример ложных выбросов
в выборке δ_i при извлечении
15-кратно встроенного секретного бита
а – отрицательные ложные выбросы,
б – положительные ложные выбросы

Модификация 3. Было проведено экспериментальное исследование возможности решения третей проблемы путем перехода от усреднения значений выборки (7) к проведению мажоритарной оценки ее значений (по большинству значений определенного

знака). Такой подход дал больший объем ошибок извлечения по сравнению с усреднением, предлагаемым в исходном варианте метода КДБ.

Исходя из этого, предлагается иная модификация метода КДБ, устраняющая проблему выбросов выборки многократного извлечения секретного бита. Модификация состоит в том, что предлагается перед выполнением усреднения (7), используя известные статистические методы, выявлять выбросы и исключать их из выборки либо осуществлять сглаживание выборки в месте выбросов. В данной работе был применен алгоритм обнаружения и исключения выбросов из выборки, изложенный в монографии [9]. Использование других методов обработки выбросов является вопросом дальнейшего исследования.

Программная реализация и экспериментальное исследование предложенных модификаций

Для экспериментального исследования предложенного усовершенствованного метода КДБ было разработана программное обеспечения выполняющее встраивание данных по классическому методу КДБ и встраивание по методу КДБ с учетом предложенных модификаций.

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, а также шум типа «соль и перец».

В ходе эксперимента производилось встраивание в выбранные изображения по классическому и модифицированному методу КДБ секретного текстового сообщения диной 80 символов. Секретное сообщение при этом выбиралось случайным образом из подготовленного набора, включающего 20 сообщений.

Результаты эксперимента оценивались в виде следующих параметров:

– наличие ошибок извлечения для контейнеров, содержащих «проблемные области»;

– количество ошибок извлечения при применении активных стеганографических атак типа JPEG-сжатие, размытие, поворот.

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. При этом стойкость к активным стенографическим атакам (сжатием с потерями, размытием и поворотом изображения-контейнера) осталась неизменной по сравнению с исходным вариантом метода КДБ.

Заключение

В данной работе предложено усовершенствование метода КДБ, выполняющего стеганографическое внедрение данных в пространственную область растрового изображения. Усовершенствование состоит во введении в метод дополнительных правил, устраняющих проблемы извлечения данных, характерные для некоторых случаев заполнения исходного графического контейнера.

За счет введения предложенных модификаций были устранены ошибки извлечения:

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

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

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

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

Стойкость усовершенствованного метода к активным стенографическим атакам осталась на уровне классического метода КДБ.

Литература

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

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

3. 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.

4. Cox, I. Digital Watermarking and Steganography [Text] / I. Cox, M. Miller, J. Bloom, J. Fridrich. – Burlington: Morgan Kaufmann Publishers, 2008. – 592 p.

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

6. Kutter, M. Digital Signature of Color Images using Amplitude Modulation [Text] / M. Kutter, F. Jordan, F. Bossen // Proc. SPIE Storage and Retrieval for Image and Video Databases. – 1997. – Vol. 3022. – P. 518-526.

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

8. Иванов, Д.В. Алгоритмические основы растровой машинной графики [Текст] / Д.В. Иванов, А.С. Карпов, Е.П. Кузьмин, В.С. Лемпицкий. – М.: Бином, 2007. – 284 с.

9. Новицкий, П.В. Оценка погрешностей результатов измерений [Текст] / П.В. Новицкий, Н.А. Зограф. – М.: Энергоатомиздат, 1991. – 304 с.

Поступила в редакцию 8.02.2013, рассмотрена на редколлегии 13.03.2013

Рецензент: д-р техн. наук, проф., проф. кафедры компьютерных интеллектуальных систем и сетей А.В. Дрозд, Одесский национальный политехнический университет, Одесса.

УДОСКОНАЛЕННЯ МЕТОДУ СТЕГАНОГРАФІЧНОГО ПРИХОВАННЯ ДАНИХ КУТТЕРА-ДЖОРДАНА-БОССЕНА

К.В. Защолкін, О.І. Іващенко, О.М. Іванова

Розглянута задача захисту інформації шляхом її стеганографічного приховання в графічному контейнері. Пропонується удосконалення методу Куттера-Джордана-Боссена, який виконує стеганографічне вбудовування даних в просторову область растрового зображення. Удосконалення полягає у введенні в метод додаткових правил, які усувають проблеми добування даних, характерні для деяких випадків заповнення первісного графічного контейнера. Наведено результати дослідження удосконаленого метода в розробленому середовищі його програмної реалізації.

Ключові слова: стеганографія, приховування даних, захист інформації, вбудовування даних, графічний стего-контейнер, просторова область стего-контейнера.

IMPROVEMENT OF THE METHOD OF STEGANOGRAPHIC INFORMATION HIDING OF KUTTER-JORDAN-BOSSEN

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

The task of protecting data by its steganographic hiding in graphic container is considered. The improvement of method of Kutter-Jordan-Bossen, which processes steganographic embedding in spatial domain of bit image, is offered. The improvement is made by insertion to the method additional rules, eliminating the problem of data extraction which is typical for certain cases of filling of the initial graphic container. The results of investigation of the improved method are shown in the developed environment of its program realization.

Key words: steganography, information hiding, information security, information embedding, graphics stego-container, spatial domain of stego-container.

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

Иващенко Александр Игоревич – 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.