УДК 651.93

Сокрытие информации в изображениях методом Куттера-Джордана-Боссена

Дымченко Оксана Александровна
Амурский государственный университет
студент

Самохвалова Светлана Геннадьевна
Амурский государственный университет
канд. техн. наук, доцент

Аннотация
Статья посвящена описанию метода цифровой стеганографии и программному продукту, который был разработан на основе метода Куттера-Джордана-Боссена. Данный метод позволяет решать задачи встраивания информации в изображение. Это метод обладает большим количеством преимуществ по сравнению с остальными методами.
Ключевые слова: шифрование, стеганография, встраивание, извлечение, пиксель, бит, сообщение

Hiding information in images by method of Kutter-Gordan-Bossen

Dymchenko Oksana Aleksandrovna
Amur State University
Student

Samokhvalova Svetlana Gennadievna
Amur State University
Candidate of technical sciences, associate professor

Abstract
The article describes the method of digital steganography and software based on method of Kutter-Gordan-Bossen. This method allows solving the problem of integrating information in the image. This method has a lot of advantages over other methods.
Key words: encryption, steganography, integration, extraction, pixel, bit, massage

Проблема защиты информации во все времена заключалась в ее сохранности и доступности только определенному кругу лиц. Для решения этих задач используются два подхода: спрятать и сделать недоступным. Со временем из первого оформилось сначала искусство, а потом и наука стеганография, а из второго – криптография.

Стеганография – это наука о скрытой передачи информации путём сохранения в тайне самого факта передачи. В отличии от криптографии, скрывающей содержание секретного сообщения, стеганография скрывает сам факт передачи скрытого сообщения.

Главная идея стеганографии – скрытная передача информации по некоторому каналу связи. Но применение этой идеи на много шире и разнообразнее простого обмена секретными посланиями. Это и защита авторских прав, коммерческих тайн, и снабжение мультимедиа объектов дополнительной информацией, и обход систем контроля информационных потоков, и создание скрытых каналов утечки информации, и скрытое использование программного обеспечения, неразрешённого к использованию.

Структура стеганографической системы приведена на рисунке 1.

Рисунок 1 – Структурная схема стегосистемы

Сокрытие внедряемых данных предъявляет серьёзные требования к контейнеру:

– размер контейнера в несколько раз должен превышать размер встраиваемых данных;

– изменения, которые будут внесены в контейнер при встраивании секретного сообщения, не должны превышать порог чувствительности среднестатистического человека и инструментов стегоанализа;

– контейнер должен сохранять свою функциональность после внедрения сообщения, то есть, если сообщение внедряется в программный код, то он должен работать так же, как работал до встраивания секретного сообщения.

Цифровая стеганография основана на сокрытии или внедрении дополнительной информации в цифровые объекты, внося искажения, которые ниже порога чувствительности человека.

Метод Куттера-Джордана-Боссена предназначен для встраивания информации в растровые изображения. Он обладает высокой пропускной способностью, устойчивостью к искажениям, устойчивостью к основным видам атак [1].

Метод Куттера-Джордана-Боссена основан на том, что зрение среднестатистического человека наименее чувствительно к синему цвету [1],

исходя из этого изменения в синем цветовом канале изображения будут меньше всего заметны. Соответственно, метод предлагает встраивание битов сообщения в синий канал контейнера в цветовой модели RGB.

Бит сообщения встраивается в канал синего цвета путём изменения значения синей цветовой компоненты выбранного пикселя.

Для начала определяется яркость пикселя контейнера по формуле (1).

$$\lambda\, x, y = 0{,}29890 \cdot R\, x, y + \ 0{,}58662 \cdot G\, x, y + \ 0{,}11448 \cdot B\, x, y\,, \qquad (1)$$

где λ x,y – яркость пикселя;

Rx,y, Gx,y, Bx,y – значения соответствующих цветовых компонент пикселя контейнера: красной, зелёной и синей [2].

Затем модифицируется значение синей цветовой компоненты выбранного для встраивания пикселя Bx,y по формуле (2).

$$B'_{x,y} = \begin{cases} B_{x,y} - v \cdot \lambda_{x,y}, & \text{при } m_i = 0; \\ B_{x,y} + v \cdot \lambda_{x,y}, & \text{при } m_i = 1. \end{cases} = B_{x,y} + (2 \cdot m_i - 1) \cdot v \cdot \lambda_{x,y} \qquad (2)$$

где v – константа, определяющая энергию встраиваемого сигнала.

Рекомендуемым значением константы считается 0,15.

Извлечение сообщения из стего в данном случае не требует наличия исходного изображения, при извлечение используют метод прогнозирования синей цветовой компоненты.

Оценочное значение яркости пикселя рассчитывается по формуле (3).

$$B_{x,y}^{\text{прог}} = \frac{1}{4\sigma}\left(\sum_{i=-\sigma}^{+\sigma} B_{x+i,y} + \sum_{j=-\sigma}^{+\sigma} B_{x,y+j} - 2 \cdot B_{x,y} \right), \qquad (3)$$

где $B^{\text{прог}}$x, y – прогнозируемое (оценочное) значение синей цветовой компоненты;

σ – количество пикселей в стороны по вертикали и горизонтали от оцениваемого. В случае креста 7x7, σ = 3.

После этого необходимо рассчитать разницу (σ) между полученным спрогнозированным значением и реальным по формуле (4).

$$\delta = B_{x,y} - B_{x,y}^{\text{прог}}. \qquad (4)$$

Если полученная разность $\delta < 0$, то извлечённый бит сообщения m = 0; если $\delta > 0$, то извлечённый бит сообщения m = 1. Разность не может быть нулевой, иначе либо значение спрогнозировано неправильно, либо неверно выбран пиксель изображения. В данном случае, извлечение является высокопроцентным.

Извлечение бита сообщения основывается на получении оценки значения синей цветовой компоненты пикселя (то есть получении её приблизительного исходного значения) и её сравнения с текущим значением синей цветовой компоненты. При этом извлечение является высоковероятным, но не стопроцентным [2]. Для решения этой проблемы было предложено кратное встраивание, то есть выполнять встраивание каждого бит сообщения τ раз. Соответственно, при извлечении для каждого бита сообщения будет получаться τ оценок значения бита секретного сообщения. Тогда секретный бит сообщения должен извлекаться по результатам усреднения разницы между реальным и оценочным значением синей цветовой компоненты всех пикселей, в которые был встроен данный бит сообщения будет находиться по формуле (5).

$$\delta = \frac{1}{\tau} \cdot \sum_{j=1}^{\tau} \left(B_{x,y} - B_{x,y}^{\text{прог}} \right) . \quad (8)$$

δ в этом случае имеет то же значение, что и при одиночном встраивании. То есть, если $\delta < 0$, то извлечён бит сообщения $m = 0$, если $\delta > 0$, то извлечён бит сообщения $m = 1$ [3].

Для повышения процента извлечения было принято решение использовать 5 встраиваний.

Несмотря на свою простоту, метод Кутера-Джордана-Боссена устойчив ко многим известным видам атак. Кроме того, к достоинствам данного метода можно отнести высокую пропускную способность, устойчивость к несанкционированному ознакомлению, устойчивость к частотному детектированию, устойчивость к разрушению младших бит контейнера, устойчивость к обрезанию краёв, устойчивость к сжатию.

Разработка программного продукта велась в среде Visual Studio 2017 на языке C#.

Для обеспечения удобства и эргономичности было разработано только главное окно, представленное на рисунке 2, выполняющее все необходимые функции.

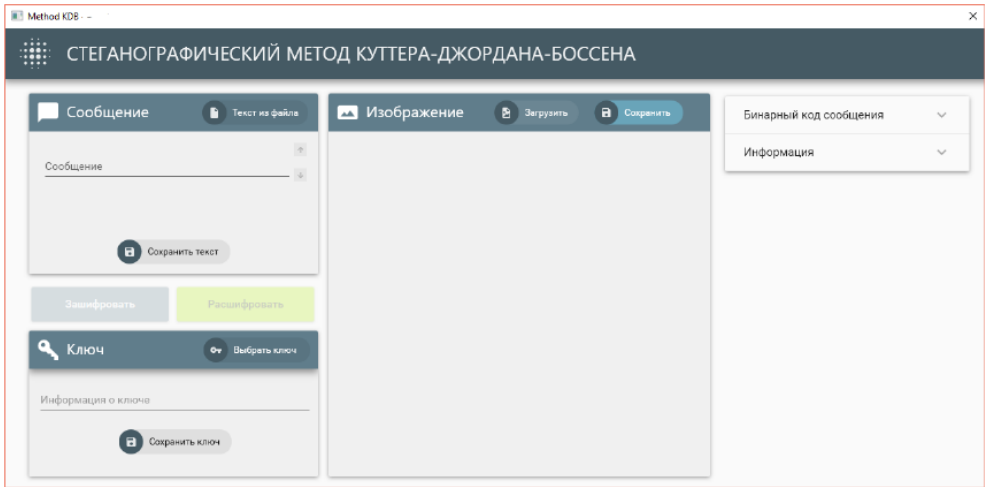

Рисунок 2 – Главное окно приложения

Помимо этого для комфорта пользователей, а также для предотвращения ошибок и утери данных были разработаны формы уведомления. Виды форм уведомления представлены на рисунке 3.

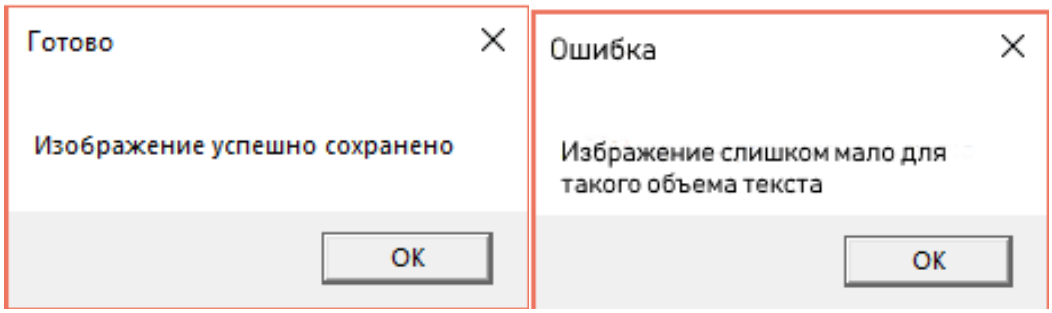

Рисунок 3 – Окна уведомления и ошибки

Для проверки качества встраивания и извлечения были проведены тестовые испытания системы. Таким образом, в данном случае тестирование разработанной программы упрощено до обычной проверки работоспособности и выполнения функций. Пример тестирования изображен на рисунке 4.

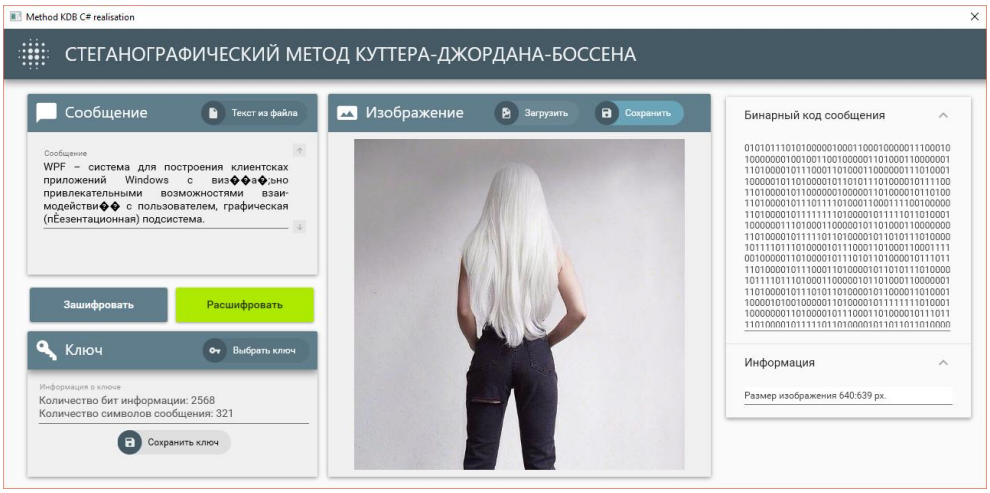

Рисунок 4 – Пример тестирования

После проведения испытаний можно сделать вывод, что ошибка извлечения в некоторых случаях доходит до 5 %.

При проведении вычислений было установлено, что средний процент верного извлечения примерно равен 97%. Для данного метода процент извлечения в данной реализации достаточно высок. Так как метод носит вероятностный характер, то обычно его средний процент верного извлечения колеблется в пределах 80-90%.

Библиографический список

1. Аграновский, А.В. Основы стеганографии: учеб. пособие для вузов

Ростов-на-Дону.: Олимп, 2003. 220 с.
2. Аграновский А.В. Практическая криптография: алгоритмы и их программирование : учеб.пособие. Спб., 2009. 250 с.
3. Коханович Г. Ф. Компьютерная стеганография. Теория и практика. К.: «МК-Пресс», 2006. 110 с.