УДК 004.056

А.В. ДОРОЖАН, асп., ХНУРЕ, Харьков,
А.А. АСТРАХАНЦЕВ, доц.,канд.техн.наук, ХНУРЕ, Харьков,
О.О. ВОВК, студ, ХНУРЕ, Харьков,

ИССЛЕДОВАНИЕ ХАРАКТЕРИСТИК МЕТОДОВ СКРЫТИЯ С ИСПОЛЬЗОВАНИЕМ НЗБ НА ФОНЕ АДДИТИВНОГО ШУМА

Досліджуються характеристики методів приховування інформації у нерухомих зображеннях на основі заміни найменш значущого біту. Оцінено характеристики методів вбудовування при використанні завадостійкого кодування на тлі адитивної гаусівської завади.
Ключові слова: НЗБ, адитивний шум, приховання інформації у нерухомих зображеннях.

Исследуются характеристики методов скрытия информации в неподвижных изображениях на основе замены наименее значащего бита. Оценены характеристики методов встраивания при использовании помехоустойчивого кодирования на фоне аддитивного гауссовского шума.
Ключевые слова: НЗБ, аддитивный шум, скрытие информации в неподвижных изображениях.

We study the characteristics of the methods of hiding information in still images based on the replacement of the least significant bit. Evaluated characteristics of the embedding methods using error correcting coding in Additive Gaussian noise.
Keywords: LSB, additive noise, hiding information in still images.

Введение

Метод наименее значащего бита (LSB) является наиболее распространенным в цифровой стеганографии. Появившийся в начале 90-х годов 20-го века, он основывается на ограниченных способностях органов чувств, вследствие чего людям очень тяжело различать незначительные вариации звука или цвета. Рассмотрим этот метод на примере 24-битного растрового RGB изображения.

Каждая точка в таком изображении кодируется 3мя байтами, каждый байт определяет интенсивность красного (Red), зеленого (Green) и синего (Blue) цвета. Совокупность интенсивностей цвета в каждом из 3х каналов определяет оттенок пикселя (рис. 1).

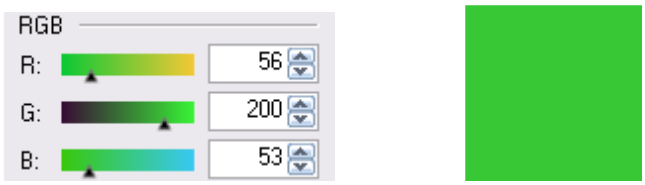

Рис.1. Пример получения оттенка в RGB изображении

Младшие разряды в меньшей степени влияют на итоговое изображение, чем старшие. Из этого можно сделать вывод, что замена одного или двух младших, наименее значащих битов, на другие произвольные биты настолько незначительно исказит оттенок пикселя, что зритель просто не заметит изменения.

Допустим, нам нужно скрыть в пикселе изображения (с параметрами R=56, G=200, B=53) шесть бит: 100111. Для этого разобьем их на три пары и заместим ими по два младших бита в каждой цветовой компоненте. Вместо пикселя с

параметрами R=56 (00111000), G=200 (11001000), B=53 (00110101), получим R=58 (00111010), G=201 (11001001), B=55 (00110111). В результате мы получим новый оттенок, очень похожий на исходный. Эти цвета трудно различить даже на большой по площади заливке (рис. 2).

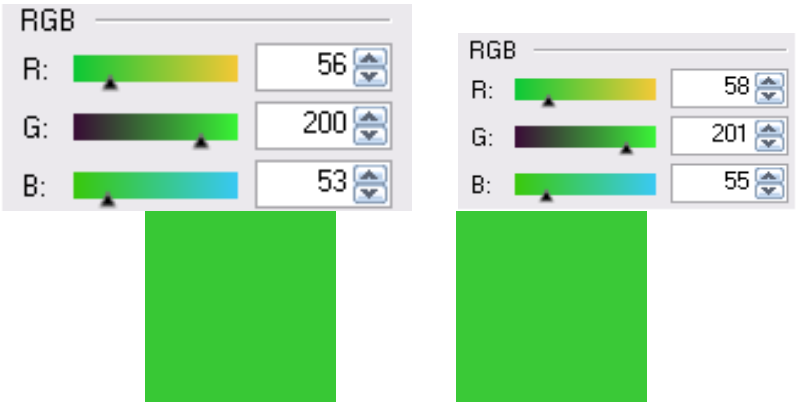

Рис. 2. Сравнение двух оттенков RGB изображения

1. Анализ возможности встраивания в 2 и более НЗБ

Замена двух младших битов не воспринимается человеческим зрением, и теоретически, в случае необходимости можно использовать и три бита, но это хотя и существенно не скажется на качестве картинки, будет легко обнаружено статистическими методами, ввиду ухудшения отношения сигнал/шум (рис. 3).

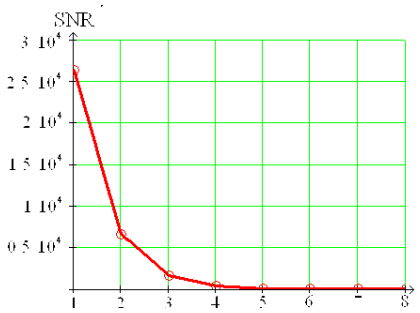

Рис. 3. Зависимость отношения С/Ш от номера модифицируемого бита

Алгоритм наименее значащего бита широко используют на практике в стеганографии, благодаря его простоте реализации, а также высокой пропускной способности передаваемой скрытой информации. Но данный алгоритм имеет целый ряд недостатков.

2. Исследование неумышленных и злонамеренных атак на стегосистему

Для исследования неумышленных атак на алгоритм НЗБ в программе Mathcad была реализована модель канала связи со встраиваемой помехой типа аддитивный гауссовский белый шум. В качестве контейнеров использовались 24-битные bmp-файлы. Исследовалось встраивание в младший бит и два младших бита.

При исследовании влияния злонамеренных атак передаваемый файл-контейнер подвергался различного вида воздействиям характерным для применяемых к изображению функциям (сжатие, изменение яркости, контраста, обрезание краев и т. п.).

На практике алгоритм НЗБ подтвердил свою полную неустойчивость к неумышленным помехам и атакам. Результаты эксперимента показали, что любые воздействия на объект затрагивающие область, в которую были встроены метки начала и конца полезного сообщения, с последующим изменением её битовой составляющей, делают невозможным не только декодирование, но и обнаружение сообщения. Изменения, вносимые аддитивной помехой, пропорциональны её амплитуде и также пагубно воздействуют на декодирование передаваемой информации (рис. 4,5).

Таким образом, были выявлены два основных недостатка данного метода:

1. Скрытое сообщение легко разрушить, например, при сжатии или обрезке исходного файла-контейнера. Либо при передаче через канал связи с высокой вероятностью возникновения помехи.

2. Не обеспечена секретность встраивания информации. Точно известно местоположение зашифрованной информации.

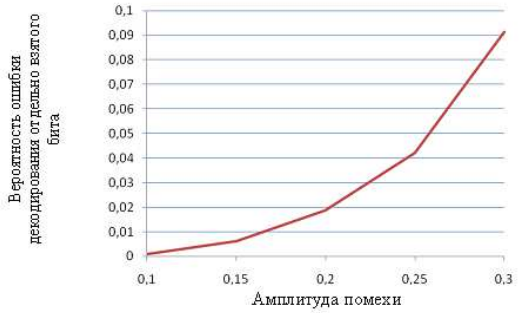

Рис. 4. Зависимость вероятности ошибки декодирования отдельно взятого бита от величины амплитуды аддитивной помехи

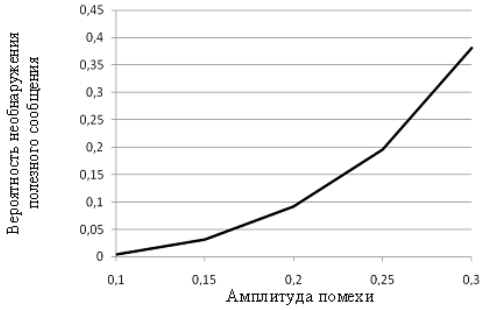

Рис. 5. Зависимость вероятности необнаружения полезного сообщения от величины амплитуды аддитивной помехи

3. Рекомендации по устранению недостатков метода

Для устранения первого недостатка не следует использовать для хранения сообщения более трех битов каждого байта контейнера, а лучше ограничиться двумя, разбив большое сообщение на несколько мелких или подобрав более емкий файл-носитель. Кроме того, не стоит забивать контейнер пользовательскими данными «под завязку» – чем меньше будет доля важной информации в общем объеме передаваемого файла, тем сложнее обнаружить факт закладки и тем меньше вероятность повреждения полезной информации при «неумышленных атаках» возникающих в результате действий производимых с графическими файлами (изменение яркости, контраста, обрезка, сжатие и т.д.). На практике обычно рекомендуют скрывать сообщения так, чтобы их размер составлял не более 10% размера контейнера. Также следует применять дублирование сообщения, помещенного в изображение-контейнер, для лучшей сохранности при изменении изображения.

Помимо этого использование самокорректирующего помехоустойчивого кодирования также должно обеспечить более высокую вероятность обнаружения и извлечения полезного скрываемого сообщения. Также для повышения вероятности обнаружения сообщения целесообразно использовать вероятностное обнаружение меток начала и конца сообщения.

Для преодоления второго недостатка можно встраивать информацию не во все пиксели изображения, а лишь в некоторые из них, определяемые по псевдослучайному закону в соответствии с ключом, известному только законному пользователю (при этом порядок следования битов в сообщении может не совпадать с порядком следования пикселей изображения-контейнера, в который вшит бит). Например: 2-й бит сообщения внедряем в седьмой пиксель

(относительно первого), 3-й бит в пятый пиксель и.т.д. Пропускная способность при этом уменьшается.

Все bmp контейнеры можно разделить на два класса: «чистые» и зашумленные. В «чистых» картинках прослеживается связь между младшим битом, который мы изменяем, и остальными 7-ю битами элементов цвета, а также прослеживается существенная зависимость самих младших битов между собой. Внедрение сообщения в «чистую» картинку разрушает существующие зависимости, что очень легко выявляется пассивным наблюдателем. Если же картинка зашумлена (например, получена со сканера или фотокамеры), то определить вложение становиться на порядок сложнее. Таким образом, в качестве файлов-контейнеров для метода LSB рекомендуется использовать файлы которые не были созданы на компьютере изначально.

На практике обычно ограничиваются поиском пикселей, модификация которых не вносит заметных искажений в изображение. Затем из этих пикселей в соответствии с ключом выбираются те, которые будут модифицироваться. Скрываемое сообщение шифруется с применением другого ключа. Этот этап может быть дополнен предварительной компрессией для уменьшения объема сообщения.

Выводы

Использование методов на основе НЗБ без дополнительной обработки не эффективно ввиду низкой стойкости к атакам различного рода. Так, изменение яркости и контраста, сжатие приводят к практически полному уничтожению встраиваемого сообщения, а атаки против стегодекодера, основанные на масштабировании, повороте и обрезке изображения приводят к несрабатыванию детектора.

Повышение надежности и помехоустойчивости данного алгоритма возможно путем применения помехоустойчивого кодирования и «мягкого» детектирования меток. Применение помехоустойчивого кода Хемминга (12,8) позволяет в среднем уменьшить вероятность ошибки на 10%. Применение мягкого детектирования позволило увеличить вероятность срабатывания детектора в среднем на 25%.

В работе впервые оценены характеристики методов на основе НЗБ на фоне аддитивного гауссовского шума. Исследования показали, что при отношении С/Ш равным 10 и выше обеспечивается вероятность ошибки порядка 10^{-3}.

Полученные рекомендации позволяют повысить перспективу использования данного метода, за счет повышения его стойкости и защищенности.

Список литературы: 1. *Аграновский А.В., Балакин А.В., Грибунин В.Г., Сапожников С.А.* Стеганография, цифровые водяные знаки и стегоанализ. – М.: Вузовская книга, 2009.**2.** *Конахович Г. Ф., Пузыренко А. Ю.* Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.**3.** *Грибунин В. Г., Оков И. Н., Туринцев И. В.* Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.

Поступила в редколлегию 17.03.2012