электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0421100025. ISSN 1994-0408

Обзор современных алгоритмов стеганографии.

77-30569/370605

 # 04, апрель 2012

Васина Т. С.

УДК 003.26.

МГТУ им. Н.Э. Баумана
tanka_best@mail.ru

Введение

Эта статья является продолжением моей предыдущей работы. В ней я рассматриваю наиболее популярные и широкоизвестные сейчас алгоритмы стеганографии и рассказываю о плюсах и минусах того или иного метода.

Для начала рассмотрим сами алгоритмы.

Все алгоритмы встраивания скрытой информации можно разделить на несколько подгрупп.

1) Работающие с самим цифровым сигналом. Примером реализации данного алгоритма может выступать метод LSB.
2) «Впаивание» скрытой информации. В данном случае происходит наложение скрываемого изображения (звука, иногда текста) поверх оригинала. Часто используется для встраивания ЦВЗ (цифровой водяной знак) .
3) Алгоритмы, связанные с особенностями форматов файлов. Сюда можно отнести запись информации в метаданные или в различные другие, не используемые зарезервированные поля файла.

Теперь рассмотрим преимущества и недостатки каждого алгоритма на примерах.

1. Метод LSB

LSB (Least Significant Bit, наименьший значащий бит) . Суть этого метода заключается в замене последних значащих битов в контейнере (изображения, аудио или видеозаписи) на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека [1].

Для простоты описания можно рассмотреть принцип работы этого метода на примере 24-битного растрового RGB-изображения. Одна точка изображения в этом формате кодируется тремя байтами, каждый из которых отвечает за интенсивность одного из трех составляющих цветов (в соответствии с рисунком 1).

Рис. 1. Представление цвета пикселя в 24-битном bmp-изображении

В результате смешения цветов из красного (R), зеленого (G) и синего (B) каналов пиксель получает нужный оттенок. Чтобы нагляднее увидеть принцип действия метода LSB, распишем каждый из трех байтов в битовом виде. Младшие разряды (на рисунке они расположены справа) 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 данной точке изображения шесть бит: 101100. Для этого разобьем их на три пары и заместим ими по два младших бита в каждом канале (в соответствии с рисунком 2).

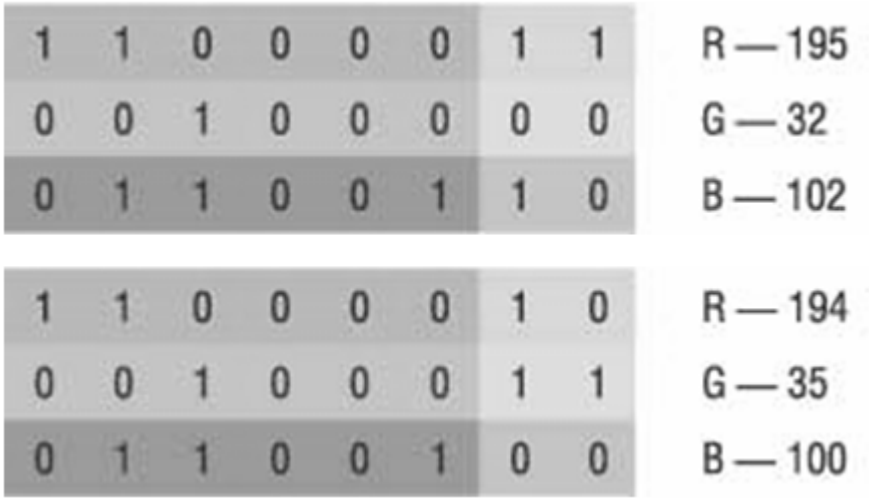

Рис. 2. Исходные и измененные компоненты цвета

Рис. 3. Цвет пикселя с внедренными данными

В результате мы получим новый оттенок, очень похожий на исходный (см. рис. 3). Эти цвета трудно различить даже на большой по площади заливке. Как показывает практика, замена двух младших битов не воспринимается человеческим глазом. В случае необходимости можно занять и три разряда, что весьма незначительно скажется на качестве картинки.

Теперь можно посчитать полезный объем такого RGB-контейнера. Занимая два бита из восьми на каждый канал, мы будем иметь возможность спрятать три байта полезной информации на каждые четыре пиксела изображения, что соответствует 25 % объема картинки. Таким образом, имея файл изображения размером 200 Кбайт, мы можем скрыть в нем до 50 Кбайт произвольных данных так, что невооруженному глазу эти изменения не будут заметны.

Все BMP контейнеры нужно разделить на два класса: «чистые» и зашумленные. В «чистых» картинках прослеживается связь между младшим битом, который подвергается изменениям, и остальными 7-ю битами элементов цвета, а также видна зависимость самих младших битов между собой. Внедрение сообщения в «чистую» картинку разрушает существующие зависимости, что очень легко выявляется наблюдателем. Если же картинка зашумлена (например, получена со сканера или фотокамеры), то определить вложение становиться намного сложнее. Таким образом, в качестве файлов-контейнеров для метода LSB рекомендуется использовать файлы, которые не были созданы на компьютере изначально [2].

Преимущества метода:

1) размер файла-контейнера остается неизменным;
2) при замене одного бита в канале синего цвета внедрение невозможно заметить визуально;
3) возможность варьировать пропускную способность, изменяя количество заменяемых бит.

Недостатки метода:

1) метод неустойчив к обработке файла-контейнера.

2. Метод встраивания ЦВЗ

Цифровой водяной знак — технология, созданная для защиты авторских прав мультимедийных файлов. Обычно цифровые водяные знаки невидимы. Однако ЦВЗ могут быть видимыми на изображении или видео. Обычно это информация представляет собой текст или логотип, который идентифицирует автора.

Стеганография применяет ЦВЗ, когда стороны обмениваются секретными сообщениями, внедрёнными в цифровой сигнал. ЦВЗ используется как средство защиты документов с фотографиями — паспортов, водительских удостоверений, кредитных карт с фотографиями. Комментарии к цифровым фотографиям с описательной информацией — ещё один пример невидимых ЦВЗ. Цифровые водяные знаки получили своё название от старого понятия водяных знаков на бумаге (деньгах, документах)[1].

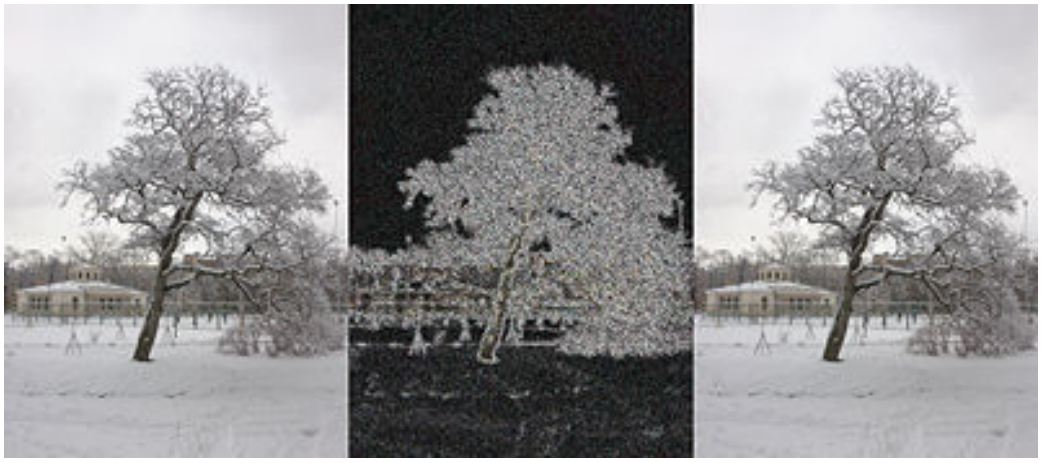

Рис. 4. Пример цифрового водяного знака (слева нормальное изображение, справа помеченное, в центре разница между изображениями с увеличенной яркостью)

Преимущества:

1) Метод не требует дополнительных процедур предобработки(в частности шифрования) изображения ЦВЗ.
2) Метод не требует использования фиксированного ЦВЗ для обнаружения модификаций, что обеспечивает стойкость ЦВЗ к различного рода атакам.

Недостатки метода:

1) ЦВЗ могут, например, позволять выполнять сжатие изображения, но запрещать вырезку из него или вставку в него фрагмента.

3. Алгоритмы, связанные с особенностями форматов файлов

Этот метод прост в реализации и зачастую не требует специального программного обеспечения. Многие распространённые методы цифровой стеганографии используют графические или звуковые файлы в качестве носителей-контейнеров. Следовательно, будет полезно сделать обзор кодирования графических и звуковых файлов перед обсуждением того, как стеганография и стегоанализ работают с этими контейнерами. Рисунок 5 показывает цветовой куб модели RGB, обычное средство для представления конкретного цвета по относительной интенсивности его трех составляющих цветов – красного, зеленого и синего – каждый со своей собственной осью. Отсутствие всех цветов даёт черный цвет, показанный как пересечение трех цветных осей в нулевой точке. Смесь 100 процентов красного, 100 процентов синего, и отсутствия зеленого цвета образует пурпурный цвет; голубой цвет – это 100 процентов зеленого и 100 процентов синего цвета без красного; а соединение 100 процентов зеленого и 100 процентов красного цвета без синего образуют желтый. Белый цвет – это наличие всех трех цветов.

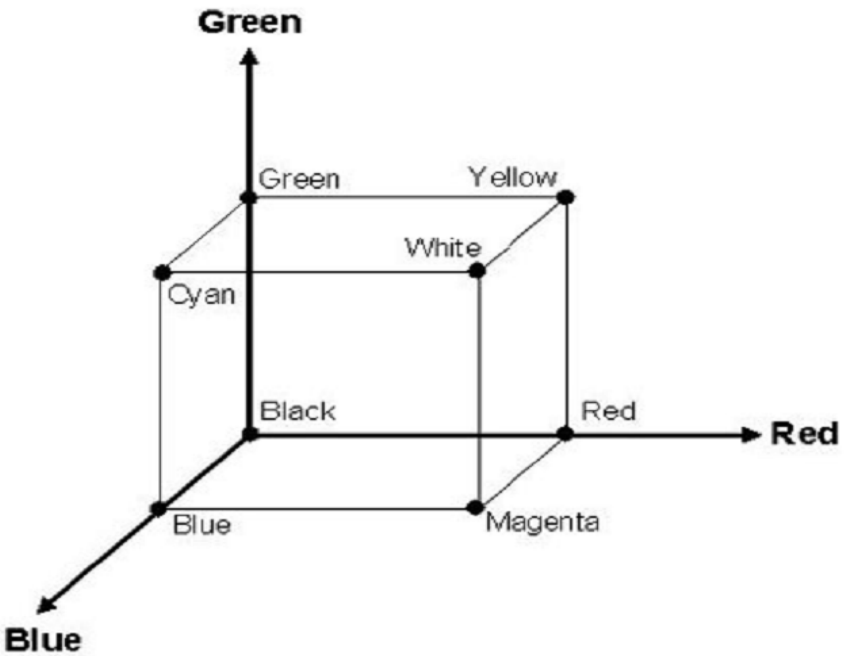

Рис. 5. Цветовой куб модели RGB

Рисунок 6 показывает уровни интенсивности (яркости) модели RGB нескольких различных цветов. Каждый компонент модели RGB задан одним байтом, поэтому значения каждой интенсивности цвета могут меняться от 0 до 255. Данный конкретный оттенок обозначен уровнем красного 191, уровнем зеленого 29 и уровнем синего 152. Затем, один пиксель пурпурного цвета будет закодирован, используя 24 бита. Эта 24-битовая схема кодирования поддерживает 16 777 216 (2^24) уникальных цветов [3].

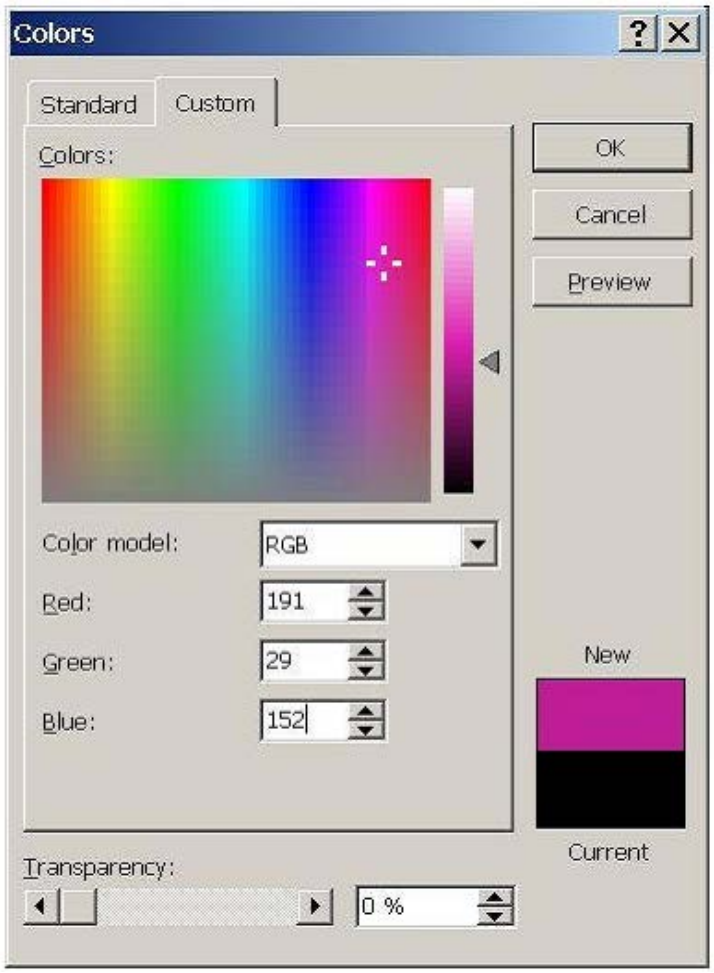

Рис. 6. Это диалоговое окно выбора цвета показывает уровни красного, зеленого и синего (RGB) данного выбранного цвета

Большинство цифровых графических приложений сегодня поддерживает 24-битовую реалистичную цветопередачу, где каждый элемент изображения (пиксел) закодирован в 24 битах, включая три байта модели RGB, как описано выше. Другие приложения кодируют цвет, используя восемь битов/пикселей. Эти схемы также используют 24- битовую реалистичную цветопередачу, но применяют палитру, которая определяет, какие цвета используются в изображении. Каждый пиксел закодирован в восьми битах, где значение указывает на 24-битовую запись цвета в палитре. Этот метод ограничивает уникальное число цветов в данном изображении до 256 (2^8) [3].

Преимущества метода:

1) простота использования;
2) простота реализации;
3) возможность скрытой передачи большого объема информации;

Недостатки метода:

1) низкая защищенность;

Заключение

Вот небольшая сравнительная характеристика тех методов, которые сейчас наиболее распространены и используются чаще всего. На основе приведенных преимуществ и недостатков читатель может подобрать себе нужный алгоритм для

Список литературы

1. AccessData. Forensic Toolkit product page [Online]. (December 29, 2003).
2. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: «МК-Пресс», 2006. — 288 с
3. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии // Защита информации. Конфидент. - 2000, № 3.- С. 26-33.

electronic scientific and technical periodical
SCIENCE and EDUCATION
EL № FS 77 - 30569. №0421100025. ISSN 1994-0408

Review of modern steganography algorithms

77-30569/370605

 # 04, April 2012
Vasina T.S.

Bauman Moscow State Technical University
tanka_best@mail.ru

This article presents a brief review of modern shorthand algorithms. Three algorithms are considered. The first one is an algorithm working with a digital signal. In the article it is described as LSB method. The second algorithm is “sealing-in” any hidden information. In the article it is presented as DWM method. And the third algorithm is connected with features of file formats. Pros and cons of each algorithm are presented, which helps to fully understand these algorithms.

Publications with keywords: steganography, algorithm, LSB, RGB, redundancy, DWM
Publications with words: steganography, algorithm, LSB, RGB, redundancy, DWM

References

1. *AccessData. Forensic Toolkit product page*. Available at: http://accessdata.com/, accessed 29 December 2003.

2. Konakhovich G. F., Puzyrenko A. Iu. *Komp'iuternaia steganografiia. Teoriia i praktika* [Computer steganography. Theory and practice]. Kiev, «MK-Press», 2006. 288 p.

3. Bykov S. F. Algoritm szhatiia JPEG s pozitsii komp'iuternoi steganografii [JPEG shrinking algorithm from a position of computer steganography]. *Zashchita informatsii. Konfident*, 2000, no 3, pp. 26-33.