электронный журнал
МОЛОДЕЖНЫЙ НАУЧНО-ТЕХНИЧЕСКИЙ ВЕСТНИК
Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл No. ФС77-51038.

УДК 004.056

Анализ модификаций стеганографического метода LSB

Перов Д.Ю., *студент*
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Программное обеспечение ЭВМ и информационные технологии»

Научный руководитель: Исаев А.Л., к.т.н., доцент
Россия, 105005, г. Москва, МГТУ им. Н.Э. Баумана,
кафедра «Программное обеспечение ЭВМ и информационные технологии»
irudakov@bmstu.ru

Метод встраивания на уровне битовой плоскости

LSB (Least Significant Bit) - это шум, поэтому его можно использовать для встраивания информации путем замены менее значащих битов пикселей изображения битами секретного сообщения. На рисунке 1 представлена работа LSB для одного значащего бита, не исключается использование и большого количества.

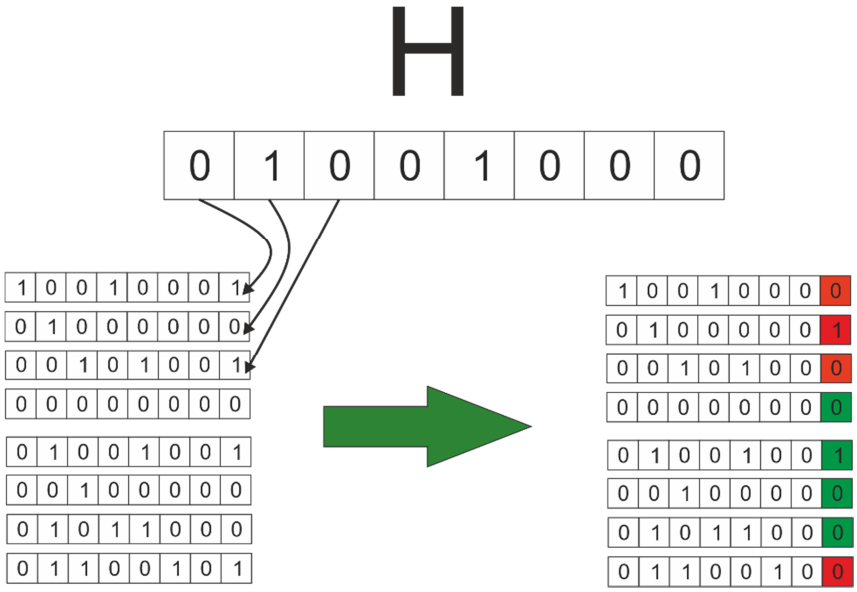

Рис.1. Пример работы LSB

Преимущества:

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:

1) неустойчив к обработке файла-контейнера.

2) легкость обнаружения и удаления

Метод Куттера-Джордана-Боссона

Использует свойство зрительной системы человека, заключающееся в слабой чувствительности к незначительному изменению яркости синего цвета.

В основе метода лежит модификации яркостей синего цвета отдельных пикселей.

Встраивание осуществляется побитно: один бит в одно значение яркости синего цветах. При этом модифицированые значения яркости синего цвета вычисляются по формуле:

$$B^*_{x,y} = \begin{cases} B_{x,y} + \lambda Y_{x,y}, \text{при } m_i = 1 \\ B_{x,y} - \lambda Y_{x,y}, \text{при } m_i = 0 \end{cases}.$$

Значение λ определяет «энергию» встраиваемого бита, то есть задает долю полноценной яркости, на которую и модифицируется канал синего цвета. Так как на принимающей стороне нет оригинального изображения, то гарантированно узнать в какую сторону изменилась яркость синего цвета мы не можем[1]. Поэтому для извлечения прогнозируется значение яркости синего цвета:

$$\overline{B_{x,y}} = \frac{\sum_{i=1}^{\sigma}(B_{x,y+i} + B_{x,y-i} + B_{x+i,y} + B_{x-i,y})}{4\sigma} \quad \text{, где } \sigma = 1 \div 3.$$

И наконец, для извлечения скрытого сообщения используется формула:

$$m_i = \begin{cases} 1, \text{при } B^*_{x,y} > \overline{B_{x,y}} \\ 0, \text{при } B^*_{x,y} > \overline{B_{x,y}} \end{cases}.$$

Достоинства метода:

1) высокая пропускная способность;

2) устойчивость к детектированию и к модификации (удалению) LSB;

3) устойчивость к некоторым стеганоатакам, в том числе к атаке сжатием.

Недостатки метода:

1) вероятностный алгоритм извлечения не гарантирует отсутствие ошибок в извлеченных данных. Применение методов помехоустойчивого кодирования предполагает внесение дополнительной избыточности, что снижает пропускную способность.

2) увеличение λ приводит к повышению достоверности извлеченного сообщения, то есть к снижению количества ошибок, однако это влечет соответствующее повышение вносимых искажений, что при этом обнаруживается визуально.

Метод псевдослучайного интервала

Подразумевает под собой изменение пикселей, задаваемых функцией/ ключом. Заключается в случайном распределении битов секретного сообщения по контейнеру, в результате чего расстояние между двумя встроенными битами определяется псевдослучайно. Эта методика особенно эффективна в случае, когда битовая длина секретного сообщения существенно меньше количества пикселей изображения.

Рассмотрим простейший случай этого метода, когда интервал между двумя последовательными встраиваниями битов сообщения является функцией координат предыдущего модифицированного пикселя[2].

Пусть имеется некоторое изображение представленное массивом яркостей отдельных пикселей, пусть секретный ключ задает псевдослучайные числа $k = \{k_1, k_2, k_3, \dots, k_n\}$, тогда пиксели с интервалами $k_1, k_2, k_3, k_4, \dots, k_n$

Пропускная способность данного метода уменьшится в среднем в N раз, где N – усредненное значение интервалов $k_1, k_2, k_3, k_4, \dots, k_n$:

$$N = \frac{1}{n}\sum_{i=1}^{n} k_i.$$

Однако это уменьшение позволяет существенно повысить устойчивость к детектированию и к извлечению сообщения. Без знания секретного ключа (множества интервалов) практически невозможно обнаружить встроенные данные, а тем более их извлечь.

Достоинства метода:

1) высокая скорость преобразования;

2) устойчивость к детектированию и извлечению сообщения.

Недостатки метода:

1) LSB (методы LSB, ПСП, ПСИ) уязвимы к разрушению сообщения посредством обнуления или псевдослучайного заполнения всех LSB контейнеров. Такие системы являются аналогами хрупкой стеганосистемы.

Метод псевдослучайной перестановки

Метод псевдослучайной перестановки (выбора), смысл которого заключается в том, что генератор ПСЧ образует последовательность индексов j1, j2,…,jm и сохраняет k-й бит сообщения в пикселе с индексом jk.

Пусть N - общее количество бит (самых младших) в имеющемся контейнере; PN(1) - перестановка чисел {1,2, ...,N}. Тогда, если у нас имеется для скрытия конфиденциальное сообщение длиной n бит, то эти биты можно просто встроить вместо бит контейнера PN(1), PN(2),…, PN(n)[2].

Функция перестановки должна быть псевдослучайной, иными словами, она должна обеспечивать выбор бит контейнера приблизительно случайным образом. Таким образом, секретные биты будут равномерно распределены по всему битовому пространству контейнера. Однако при этом индекс определенного бита контейнера может появиться в последовательности более одного раза и в этом случае может произойти "пересечение" - искажение уже встроенного бита. Если количество бит сообщения намного меньше количества младших бит изображения, то вероятность пересечения является незначительной, и искаженные биты в дальнейшем могут быть восстановлены с помощью корректирующих кодов.

Вероятность, по крайней мере, одного пересечения оценивается как

$$p \approx 1 - \exp\left[-\frac{l_m(l_{m-1})}{2l_c}\right], l_m \ll l_c.$$

Достоинства метода:

1) Высокая пропускная способность (такая же, как и у метода LSB). ПСП является лишь предварительным кодированием перед реализацией встраивания данных. То есть сохраняет все достоинства метода-прототипа.

2) Для больших n (~1000) существенно возрастает устойчивость к детектированию, в первую очередь, статистическими методами. Однако повышение n ведет к резкому повышению сложности реализации.

Метод блочного сокрытия

Метод блочного скрытия – еще один подход к реализации метода замены. Суть этого метода заключается в следующем: изображение-оригинал разбивается на l_M непересекающихся блоков Δ_i $(1 \le i \le l_M)$ произвольной конфигурации, для каждого из которых вычисляется бит четности $b(\Delta_i)$ [1]:

$$b(\Delta_i) = \sum_{j \in \Delta_i}^{mod\ 2} LSB(C_j).$$

В каждом блоке производится скрытие одного секретного бита M_i. Если бит четности $b(\Delta_i) \neq M_i$, то происходит инвертирование одного НЗБ из блока Δ_i, в результате чего $b(\Delta_i) = M_i$.

Достоинства метода:

1) возможность модифицировать значение такого пикселя в блоке, изменение которого приведет к минимальному изменению статистики контейнера;

2) влияние последствий встраивания секретных данных в контейнер можно уменьшить за счет увеличения размера блока.

Недостатки:

1) низкая устойчивость к искажениям.

Вывод

Реальные стеганосистемы являются результатом компромисса между требуемой достоверностью и величиной вносимых искажений. На сегодняшний день существует огромное количество стеганографичечких методов, позволяющих скрывать конфиденциальную информацию внутри различных источников, но как правило большинство из них малоэффективны, либо легко обнаружимы.

Из этого следует вывод, что рассмотренные методы эффективны лишь при

небольшом количестве информации, если попытаться зашифровать больше информации, то контейнер (в данном случае изображение) сильно искажается и нарушается палитра данного изображения.

Список литературы

1. Грибунин, В. Г. Цифровая стеганография. М.: СОЛОН-Пресс, 2002. 272 с.
2. Конахович Г.Ф., Пузыренко А.Ю.. Компьютерная стеганография. Теория и практика. Киев: МК-Пресс, 2006. 288 с.
3. Миано Дж. Форматы и алгоритмы сжатия изображений в действии. М.: Триумф, 2003. 336 с.