Маскировка данных в пространственной области неподвижных изображений

Данилычев Иван Алексеевич

Студент

Факультет прикладной математики и физики МАИ, Москва, Россия

E-mail: eveningsteps@gmail.com

Проблема маскировки информации частично решается методами стеганографии: данные встраиваются в контейнер, не привлекающий внимания. Секретность системы защиты содержится в ключе — фрагменте информации, который, как правило, предварительно разделен между сообщающимися сторонами. В качестве контейнера зачастую выступает неподвижное изображение, что обусловлено рядом причин, связанных как с природой оцифрованных изображений, так и с особенностями человеческого зрения, такими как слабая чувствительность человеческого глаза к незначительным изменениям цветов изображения, его яркости, контрастности, наличии в нем шума [1].

В настоящей работе рассматривается реализация нескольких возможных методов маскировки данных, начиная с алгоритмов выбора несущих информацию пикселей, а именно — методов псевдослучайного интервала и псевдослучайной перестановки.

Метод псевдослучайного интервала является модификацией широко известного метода наименее значимого бита (least significant bit, LSB) и заключается в получении псевдослучайной последовательности приращений координат пикселей изображения, в которые будет произведено встраивание. В простейшем случае координатная функция вычисляет сумму бит в двоичном представлении прошлой координаты.

Модификацией данного алгоритма является метод псевдослучайной перестановки, где псевдослучайная последовательность состоит уже из координат целевого изображения. В [2] предлагается следующий способ генерации последовательности. Пусть x и y — две равные части строки данных, K — ключ, H — секретная хэш-функция. Разделим ключ на четыре равные части и применим следующий алгоритм:

$$\begin{aligned} y &= y \oplus H(K_1|x), \\ x &= x \oplus H(K_2|y), \\ y &= y \oplus H(K_3|x), \\ x &= x \oplus H(K_4|y). \end{aligned} \tag{1}$$

После чего значение $x + y$ будет являться следующим псевдослучайным индексом. Кроме того, для расчёта индексов можно использовать линейные конгруэнтные генераторы, полагая, что

$$x_{n+1} = (ax_n + c) \bmod m. \tag{2}$$

Помимо перечисленных алгоритмов, рассмотрен метод замены палитры [3]. Каждому пикселю изображения ставится в соответствие индекс, которому соответствует один из цветов изображения. При скрытии цвет текущего обрабатываемого пикселя заменяется на такой ближайший цвет, маскированное битовое представление которого уже содержит скрываемый фрагмент.

Также приведён метод квантования, основанный на межпиксельной зависимости. В простейшем случае для смежных пикселей строится таблица разностей, каждой из которых соответствует фрагмент двоичных данных. Аналогично методу замены палитры, цвета смежных пикселей при маскировке заменяются на такие, разница Δ_i которых соответствует маскируемым данным.

Перечисленные методы реализованы на языке C++ с применением фреймворка Qt. Для оценки качества работы стеганографических алгоритмов использован ряд метрик, типичных для анализа качества изображений и дающих количественную оценку: средняя абсолютная разность, среднеквадратичная ошибка, L^p-норма и отношения «сигнал-шум» и «максимальный сигнал-шум».

Литература

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. К.: МК-Пресс, 2006. С. 73–75
2. Luby M., Rackoff C. How to construct pseudorandom permutations from pseudorandom functions //SIAM Journal on Computing. – 1988. – Т. 17. – №. 2. – С. 373–386
3. Аграновский А. В., Балакин А. В., Грибунин В. Г., Сапожников С. А. Стеганография, цифровые водяные знаки и стегоанализ: Монография. М.: Вузовская книга, 2009. С. 139–140.