

КОРРЕКТИРОВКА ВКРАПЛЕНИЙ НА ОСНОВЕ МАРКОВСКИХ МОДЕЛЕЙ В ЗАДАЧАХ СТЕГАНОГРАФИИ

Пьянов В. В., Харин Ю. С.

*БГУ, НИИ прикладных проблем математики и информатики,
факультет прикладной математики и информатики, Минск, Беларусь,
e-mail: fpm.pyanov@bsu.by, kharin@bsu.by*

Стеганография широко применяется для обеспечения защиты информации в интернете. Главная цель стеганографии – скрыть факт передачи сообщения, однако чаще всего математический анализ сообщения может обнаружить вкрапления, показав статистические отклонения, поэтому необходимо сохранять исходную статистику сообщения при встраивании. Для этого мы рассматриваем локальную корректировку статистики после встраивания, которая возможна в случае встраивания скрытого сообщения в наименее значащие биты изображения. Локальная корректировка не меняет всю последовательность, а заменяет только биты в некоторой окрестности от мест встраивания.

Рассмотрим математическую модель вкраплений, следуя[1].

Алгоритм локальной корректировки основывается на статистике:

$$\Lambda(y) = \sum_{v_0, v_1 \in \{0,1\}} \frac{(f_{v_0, v_1} - f_{v_0} p_{v_0, v_1})^2}{f_{v_0} p_{v_0, v_1}}, \quad (1)$$

где f_{v_0, v_1} – вычисленные по наблюдаемой последовательности длины T частоты биграмм (v_0, v_1) , а p_{v_0, v_1} – вероятность появления биграммы (v_0, v_1) .

Теорема 1. Критерий проверки гипотез о наличии вкраплений асимптотического уровня значимости α задается критической областью

$$\chi_{1\alpha} = \{y \in \{0,1\}^T : \Lambda(y) \geq \chi_{1-\alpha, 2}^2\}, \quad (2)$$

здесь $\chi_{1-\alpha, 2}^2$ – квантиль уровня $1 - \alpha$ распределения χ^2 с числом степеней свободы 2.

Разработанный алгоритм локальной корректировки производит перебор всех возможных значений окрестностей точек встраивания и выбирает те значения окрестностей, на которых статистика (1) минимальна. Алгоритм производит корректировку до тех пор, пока принимается гипотеза о наличии вкраплений.

Литература