СИСТЕМА ТЕСТИРОВАНИЕ АЛГОРИТМОВ СТЕГАНОГРАФИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Щёголев Ю.Е.

Одинец Д.Н. – к.т.н., доцент

Стеганография – способ передачи информации путем сохранения в тайне самого факта передачи. В современном мире стеганографию применяют не только для секретной передачи сообщения, но и для создания цифровых подписей с целью подтверждения авторских прав. Существует множество стеганографических алгоритмов для сокрытия данных в разных форматах файлов, однако все они в той или иной степени подвержены взлому.

На сегодняшний день существуют десятки способов выявить наличие стеганографического сообщения в файле изображения, это так называемые методы стегоанализа. Однако большинство из них относятся к категории атак на стеганографические системы. Самыми популярными из них являются: RS, повышение LBS, атака по известному заполненному контейнеру и т.д. Слово «атака» в данном контексте обозначает то, что методы выявления сообщений работают только с обработанным изображениями (оригинал остается неизвестен) и выдают процент вероятности наличия зашифрованного сообщения. К недостаткам таких способов выявления относится то, что большинство атак рассчитаны на идентификацию какого-то определенного алгоритма стеганографии и бесполезны для остальных.

Если человек разрабатывает новый стеганографический алгоритм, то ему необходимо знать, насколько его метод является стойким к потенциальному стегоанализу. Цель данной работы – разработать метод для оценки стойкости стего-алгоритма.

В отличие от существующих методов стегоанализа, новый метод основан на статическом сравнении обработанного изображения с оригиналом.

Сравнение оригинального изображения с изображением, пропущенным через стегоканал, осуществляется по 17-ти различным критериям. Данные критерии сравнения делятся на 3 группы:

1. Разностные показатели искажений (максимальная разность, средняя абсолютная разность, лапласова среднеквадратическая ошибка и т.д.);
2. Корреляционные показатели искажений (нормированная взаимная корреляция, качество корреляции);
3. Прочие (структурное содержание, сигма-отношение «сигнал / шум» и т.д.);

Сравнение по каждому из критериев изображения происходит попиксельно. В качестве примера рассмотрим критерий «Средняя абсолютная разность», который вычисляется по формуле:

$$AD = \frac{1}{X \cdot Y} \sum_{x,y} |C_{x,y} - S_{x,y}|,$$

где $C_{x,y}$ – пиксель пустого контейнера (оригинального изображения), $S_{x,y}$ – пиксель заполненного контейнера (изображение после обработки).

В таблице 1 представлены примеры сравнения 2-ух алгоритмов стеганографии (наименьшего значащего бита, замены палитры).

Таблица 1. Результаты сравнения изображения, пропущенного через стегоканал, с оригиналом

Критерий	Оригинальное изображение	Алгоритм	
		НЗБ	Замены палитры
Максимальная разность	0	1	3
Средняя абсолютная разность	0	0.494	$9{,}827 \cdot 10^{-3}$
Нормированная средняя абсолютная разность	0	$3{,}823 \cdot 10^{-3}$	$7{,}611 \cdot 10^{-5}$
Среднеквадратическая ошибка	0	0.494	0.017
Нормированная среднеквадратическая ошибка	0	$2{,}010 \cdot 10^{-5}$	$7{,}084 \cdot 10^{-7}$
L_p – норма	0	0.703	0.132
Качество изображения	1	0.999980	0.999999
Нормированная взаимная корреляция	1	0.999439	0.999942
Нормированное отношение «сигма / ошибка»	256	60	0.241
Подобие гистограмм	0	3918	184

Очевидно, что чем больше критерий обработанного изображения отличается от оригинала, тем алгоритм является более стойким к стегоанализу и тем больше изображение отличается от оригинала визуально.

Список использованных источников:

1. Грибунин, В.Г. Цифровая стеганография/ В. Г.Грибунин,Оков И.Н., Туринцев И.В. М.: Солон-Пресс, 2009. 265 с..
2. Fridrich J. Steganography in Digital Media / J.Fridric, – Cambridge University Press, 2009. – 437 с.