

УСТОЙЧИВОСТЬ СТЕГАНОГРАФИЧЕСКИХ ПРЕОБРАЗОВАНИЙ К МЕТОДАМ СТЕГОАНАЛИЗА

М.Г. Савельева, И.А. Песецкий, Н.А. Песецкий

*Учреждение образования «Белорусский государственный
технологический университет», Минск, Беларусь*

Основной целью стеганоанализа является моделирование стеганографических систем и их исследование для получения качественных и количественных оценок надежности использования стеганообразования, а также построение методов выявления скрываемой в контейнере информации, ее модификации или разрушения [1].

Для анализа были выбраны следующие методы скрытия сообщения в растровых файлах: DCT и DWT. Дискретное косинусное преобразование (DCT) – это математическое преобразование, которое преобразует последовательность чисел в набор косинусоидальных компонент. Дискретное вейвлет-преобразование (DWT) – это метод анализа сигналов, который позволяет разложить сигнал на составляющие различных масштабов и частот. В стеганографии DWT часто используется для внедрения секретной информации в изображения. Этот метод позволяет скрыть данные в изображении таким образом, чтобы изменения были минимальны и незаметны для человеческого глаза. Для анализа были выбраны методы «Хи-квадрат» (χ^2) атак и атака на основе корреляционного анализа (Correlation Analysis Attack), которые позволяют узнать вероятность того, что в растровом изображении есть скрытое сообщение [2].

После проведенного исследования можно сделать вывод, что для рассмотренных методов атака χ^2 неспособна полностью обнаружить сообщение и его реальный размер, однако предполагаемый размер сообщения возрастает вместе с реальным. То есть чем больше внедренное сообщение, тем больше вероятность его обнаружения с помощью данной атаки. Тем не менее, несмотря на рост объема данных, способность χ^2 атаки к обнаружению скрытых сообщений остается менее эффективной по сравнению с САА-атаками. В случае малого и большого объема скрытой информации способность корреляционных атак обнаруживать скрытые сообщения ограничена. Однако при достаточном объеме внедренной информации, который можно назвать «оптимальным», эффективность атаки достигает максимума. Это свидетельствует о сбалансированной комбинации между статистическими аномалиями и объемом информации, что делает обнаружение сообщения сложным. При слишком малом и слишком большом объеме внедренной информации эффективность данной атаки снижается.

Исследование подтверждает, что метод DWT обладает более высокой устойчивостью и незаметностью при скрытии сообщений в растровых изображениях по сравнению с DCT. При этом атака на основе корреляционного анализа является наиболее эффективным методом для обнаружения скрытых сообщений в таких изображениях.

Список литературы

1. Исследование устойчивости стеганографии в изображениях / Е. Г. Жиляков [и др.] // Экономика. Информатика. – 2014. – Т. 29, № 1-1 (172). – С. 168–174.
2. Разинков, Е. В. Стойкость стеганографических систем / Е. В. Разинков, Р. Х. Латыпов / Ученые записки Казан. гос. ун-та. – 2009. –Т. 151, № 2.