ИССЛЕДОВАНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ, ВСТРОЕННЫХ МЕТОДОМ DEW, НА УСТОЙЧИВОСТЬ К ОПРЕДЕЛЕННЫМ ВИДАМ АТАК

А.С. Гераськин, А.А. Шуликина, А.А. Лукьянова

Развитие компьютерных технологий придали новый импульс развитию и совершенствованию нового направления в области защиты информации – компьютерной стеганографии. Одна из областей применения методов компьютерной стеганографии, которые получили широкое распространение, стали методы встраивание цифровых водяных знаков (ЦВЗ) и цифровых отпечатков пальцев, предназначенных для защиты авторских и имущественных прав на цифровую информацию различного рода.

Современные системы компьютерной стеганографии используют в качестве контейнеров растровые графические изображения различных форматов. Самое широкое распространение в последнее время получил формат JPEG.

Существует множество методов, основанных на внедрение ЦВЗ в коэффициенты матрицы дискретно-косинусного преобразования (ДКП). Наиболее интересным является метод дифференциального встраивания энергии (DEW). Его идея заключается в выборочном отбрасывании части высокочастотных коэффициентов ДКП изображений и видеоизображений, в которые можно осуществить встраивание дифференциального энергетического водяного знака [1].

Целью данной работы является исследование ЦВЗ, встроенных методом DEW, на устойчивость к определенным видам атак. Для достижения этой цели было разработано программное обеспечение, которое проводило атаки на базу, содержащую изображения с ЦВЗ, встроенными методом DEW. Были реализованы следующие группы атак: атаки, направленные на удаление ЦВЗ; геометрические атаки; криптографические атаки и атаки против используемого протокола.

Для оценки устойчивости цифрового водяного знака применялись коэффициент Пирсона и подсчет процента побитового совпадения между внедренным и извлеченным ЦВЗ.

В процессе анализа устойчивости ЦВЗ встроенных методом DEW к атакам были получены следующие результаты: Геометрические атаки: обрезка – коэффициент Пирсона ≈0.5; масштабирование – коэффициент Пирсона < 0,1; поворот – коэффициент Пирсона ≈0..5.

Статистические атаки: сжатие – коэффициент Пирсона >= 0,5; шумоподавление – коэффициент Пирсона >0.3; внесение шума – коэффициент Пирсона > 0,5. Внедрение нового ЦВЗ – коэффициент Пирсона > 0,5.

На основе полученных результатов, был сделан вывод, что метод DEW можно считать в достаточной мере устойчивым ко многим видам воздействий на контейнер. Однако, в результате исследования был сделан вывод: для повышения эффективности, методы встраивания ЦВЗ нужно осуществлять в области средних частот, а не высоких, что повысит устойчивость ЦВЗ.

Литература

1. Иваненко В.Г., Ушаков Н.В. Защита изображений формата JPEG при помощи цифровых водяных знаков // Безопасность информационных технологий. 2018. № 2. С. 106–113.