ИСПОЛЬЗОВАНИЕ КРИТЕРИЯ ХИ-КВАДРАТ ДЛЯ АНАЛИЗА СТЕГОСИСТЕМ С АУДИОДАННЫМИ

И.Л. Чваркова
Научный руководитель – к.т.н., доцент ***В.С. Садов***
Белорусский государственный университет

В настоящее время доминирующую роль среди средств контроля и разграничения доступа к информации играет шифрование или кодирование сообщений с использованием методов криптографии, которые, как правило, изменяют ее первоначальное представление и делают невозможным ее чтение, если неизвестен ключ или алгоритм кодирования. Однако во многих странах мира существует запрет на использование криптографических алгоритмов, что вынуждает искать другие пути защиты информации. Методы стеганографии позволяют передавать конфиденциальную информацию таким образом, что скрывается сам факт передачи. Цифровая стеганография – наука о незаметном и устойчивом к атакам скрытии одних данных в других. Одним из популярных методов внедрения информации является метод замены младших значащих битов, основывающийся на неспособности человека визуально заметить изменение в одном бите. Этот метод используют популярные в настоящее время программы S-Tools, EzStego, Jsteg. Младший значащий бит (LSB) несет в себе меньше всего информации. Как правило, встраивание сообщения происходит не во все младшие биты аудио-контейнера, а только в выбранные по определенному ключу, известному только законному пользователю, что обеспечивает секретность встраивания информации. Правильный выбор ключа повышает устойчивость стегосистемы к всевозможным атакам нарушителей.

Перспективным методом обнаружения скрытого сообщения в статических изображениях является проверка статистики Хи-квадрат [1]. Целью исследований была проверка применимости критерия Хи-квадрат для аудио-контейнеров. Аудио-файлы были разбиты на классы: обычная музыка (эстрадные песни, простые музыкальные фрагменты), электронная музыка, речь (стихи, стихи с небольшими фрагментами музыки). В каждом классе для каждого аудио-файла синтезирован соответствующий аудио-файл со скрытым сообщением (стего) методом замены младшего значащего бита. Критерий Хи-квадрат основывается на предположении о равных вероятностях появления соседних уровней громкости отсчетов в стего-файле, то есть при стегокодировании вероятности появления соседних уровней громкости отсчетов усредняются. Для каждого блока аудио-файла, составляющего один процент от его размера, получены значения статистики Хи-квадрат и по ним вычислены вероятности нахождения стего. В докладе представлены графические зависимости вероятности нахождения скрытого сообщения для заполненных и незаполненных контейнеров различных классов аудио-файлов. Выявлены граничные условия и приведена оценка применимости данного критерия для анализа аудиоданных. Сделан вывод о том, что критерий Хи-квадрат позволяет в лучшей степени выявить факт наличия скрытого сообщения при использовании в качестве контейнера аудио-файлов, особенностью которых является неплотный звук с большим количеством пауз, например, речевой файл. Для этого класса аудио-файлов вероятность нахождения стего в заполненной части контейнера равнялась единице, а в незаполненной части была равна нулю. В меньшей степени использование критерия Хи-квадрат позволяет обнаруживать скрытую информацию в случае аудио-контейнеров в виде плотной, богатой различными значениями уровней громкости музыки, например, классической и электронной, а также, если скрываемое сообщение рассредоточено по контейнеру небольшими “порциями” по псевдослучайному закону. В этом случае, вероятность нахождения скрываемого сообщения для заполненной части контейнера была строго равна единице, а для незаполненной части - изменялась от нуля до единицы, что затрудняет объективную оценку обнаружения стего.

Литература

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография – М.:СОЛОН-Пресс,2002.-272с. (Серия ‘Аспекты защиты’)