НОВЫЕ МЕТОДЫ СТЕГАНОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

С.А. БОГДАНОВ, Л.И. МИНЧЕНКО

Разработанная система стеганографической защиты информации использует аудиофайлы в качестве контейнеров.

Обычно стеганография используется с целью сделать маловероятным обнаружение самого факта передачи данных, а также решать задачи помехоустойчивой аутентификации, защиты от несанкционированного копирования, отслеживания распространения информации по сетям связи, поиска в мультимедийных базах данных.

Цифровые аудио записи представляют из себя матрицу амплитуд. Амплитуда — это единичный элемент звука. Он имеет фиксированную разрядность двоичного представления. Например, амплитуды звукового файла кодируются 16 битами (значения изменяются от 0 до 65534).

Младший значащий бит аудио несет в себе меньше всего информации. Известно, что человек обычно не способен заметить изменение в этом бите. Фактически, он является шумом. Поэтому его можно использовать для встраивания информации. Таким образом, для звука объем встраиваемых данных может составлять 1/16 объема контейнера. Если модифицировать два младших бита (что также почти незаметно), то можно скрытно передать вдвое больший объем данных.

В разрабатываемом программном средстве в качестве контейнеров используются файлы медиа-форматов wav, ogg vorbis. В общем случае с помощью программного средства производится преобразование защищаемого файла в массив байтов, после чего он после анализа значений амплитуд звукового файла встраивается в wav/ogg-файл.

Внедрение массива байтов, полученного из защищаемого файла, в массив байт, полученный из медиа файлов типов wav, ogg осуществляется путем последовательной замены значений младших битов слов массива, полученного из аудио-файла, значениями массива, полученного из защищаемого файла. Для реализации битовых операций, не поддерживаемых в Java непосредственно, используется операция XOR и восемь байтовых «масок», содержащих нули во всех позициях, кроме одной. Таким образом, получается запись аналогичная «BigEndian».