УДК 519.688:004.772:004.773

Гринишак А.С.
Днепропетровский национальный университет им. О. Гончара

Информационная система скрытой передачи сообщений

На данном этапе развития информационных технологий очень остро стоит проблема защиты информации от несанкционированного доступа. Каждый человек хочет защитить свою конфиденциальную информацию, которая представляет определенную ценность для него.

Существует множество программных пакетов, которые основаны на криптографических методах защиты информации. Но в ряде случаев владельцу информации необходимо скрыть факт передачи сообщения, и для этого он применяет программы, в основе которых лежат стеганографические методы сокрытия данных.

Разработанное программное обеспечение использует комбинацию способов защиты информации: криптографический — исходное сообщение шифруется и становится непонятным для человеческого восприятия, стеганографический — зашифрованный текст помещается в контейнер (изображение), и таким образом скрывается факт передачи сообщения.

Структурная схема разработанной системы изображена на рис. 1.

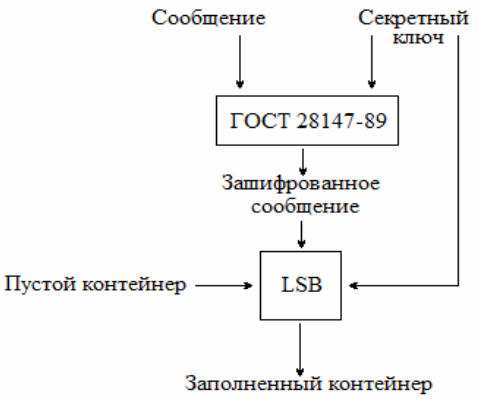

Рис. 1. Структурная схема разработанной программы

В качестве криптографической защиты используется блочный алгоритм шифрования ГОСТ 28147-89, криптостойкость которого проверена годами [2]. Реализованный алгоритм позволяет зашифровать файл любого расширения и любой длины.

Стеганографическую защиту обеспечивает наиболее известный метод сокрытия информации — LSB (Least Significant Bit) [1]. Суть реализованного метода состоит в том, что наименее значащие биты контейнера будут заменены на биты скрываемого сообщения. Биты сообщения будут записаны в определенной последовательности: для атрибутов изображения width и height система генерирует с помощью двух линейных конгруэнтных генераторов с различными параметрами две псевдослучайные последовательности соответствующей длины, которые состоят из значений, не превышающих вышеуказанные атрибуты. В качестве затравки для этих генераторов используются определенные биты секретного ключа. Это, в свою очередь, обеспечивает более стойкую защиту системы.

Программное обеспечение реализовано на языке программирования Python3. Выполнение программы возможно под любыми операционными системами: Linux, Windows или Mac OS.

Особенностью разработанной системы является то, что каждый из алгоритмов реализован в виде отдельных классов, что позволяет использовать каждый метод отдельно, независимо от другого. В результате работы программного обеспечения размер выходного файла соответствует размеру пустого файла-контейнера. Отличия между пустым и заполненным контейнерами незаметны для человеческого глаза.

Для более удобного использования системы предусмотрен простой графический интерфейс, а также интерфейс командной строки, что позволяет использовать ее из других программных пакетов.

Список использованной литературы

1. *Конахович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. - М.: МК-Пресс, 2006. - 288 с.*
2. *Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исходные тексты на языке Си. - 2-е издание. - М.: Диалектика, 2003. - 610 с.*