**BC/NW 2017 № 1 (30):12.2**

**АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ**

Благов В.Д.

XXI век славится быстрым развитием компьютерных технологий. Но как в условии этого развития можно "спрятать" личную информацию? На помощь приходит стеганография. Стеганографические методы использовались еще до нашей эры, известны случаи, когда зашифрованное сообщение наносили на дощечку до покрытия воском, сохраняя, таким образом, запись в тайне.

Целью данной статьи стал анализ современных стеганографических методов.

В масштабах данной работы был проведен анализ литературы посвященной стеганографии, а также выявление плюсов и минусов методов стеганографической шифровки информации.

В перечень рассмотренных методов попали: Методы сокрытия информации в текстовых файлах, методы шифровки в аудио/видео файлах, а также, методы сокрытия информации в графических файлах.

Для того чтобы подробнее ознакомиться с методами, необходимо разобрать что такое стеганография, как выглядит стегомодель и определить компоненты в ней.

Стеганография – это наука о сокрытии информации, методом сохранения в тайне самого факта обмена информацией.  Слово «стеганография» происходит от греческого steganos (секрет, тайна) и graphy (запись), что буквально переводится как «тайнопись».  Главное отличие стеганографии от криптографии состоит в том, что скрывается не только сообщение, но и информация о передаче сообщения. Также стеганография существенно отличается от криптографии тем, что при стеганографических методах шифрования сообщение встраивается в изображение, аудиозапись или текст, то есть в безобидный объект, который не привлекает внимание злоумышленников. В криптографии же, наличие самого зашифрованного текста вызывает подозрения.

Наиболее эффективным методом шифрования является совмещение криптографии и стеганографии.

Стеганографическая система или стегосистема – это совокупность методов формирования скрытого канала для передачи информации.

**
Рис1. Обобщенная модель стегосистемы**

Рассмотрим подробнее элементы стеганографической системы.

Контейнер – информация, в котором стеганографическим алгоритмом скрыто сообщение.

Встраиваемое сообщение – шифруемое сообщение, которое помещается в контейнер.

Ключ – секретный алгоритм, необходимый для шифрования информации.

Стегоканал – канал для передачи зашифрованной информации.

**Стеганографические методы защиты информации.**

При использовании стеганографических методов защита информации происходит на трех уровнях:

1) Неизвестен сам факт обмена информацией;

2) Неизвестен ключ;

3) Неизвестен алгоритм шифрования информации.

Наиболее распространенным являетсяметод встраивания секретной информации в тексты.

Этот метод делится на два типа:

1) Синтаксическое встраивание скрытой информации.

Сокрытие информации происходит путем изменения количества пробелов, табуляции, изменение межстрочных интервалов, использование невидимых символов, регистр букв и т.д. Синтаксические методы легко встраиваются в любой текст, вне зависимости от его языка и содержания, они довольно просты в разработке. Существенным недостатком данных методов является то, что нельзя передать большой объем секретной информации, а также они легко взламываются.

2) Лексическое встраивание скрытой информации.

Это системы, основанные на лексической структуре текста. Например, существует метод первой буквы, когда в первую букву каждого слова кодируется шифр. Одну и ту же комбинацию символов может кодировать несколько букв. Таким образом, пользователь может закодировать комбинацию 111 в слова, начинающиеся с буквы «Г», «Е» и  «Д». Такой метод дает оператору больше свободы действия при придумывании стегосообщения, текст не будет смотреться нелепо. Это преимущественно отличает данный метод от метода переменной длины. В этом методе, слова, которые вводит пользователь, должны соответствовать длине, задаваемой программой-помощником. Таким образом, определенной длине слова соответствует определенная комбинация бит. В одно слово, обычно, кодируется два бита информации из стегосообщения. Например, слова состоящие из 5-10 символов могу означать комбинацию «00», из 3-7 – «01», 4-8 – «10», 6-9 –«11», слова меньше 3 символов и больше 11 можно использовать в качестве грамматической связки и вставлять куда угодно в тексте, программой они будут игнорироваться.

Следующий рассмотренный метод: метод встраивания информации в графические файлы.

Преимущество этого метода состоит в том, что при использовании графических файлов, можно встраивать не только текст, но и изображения и другие файлы. Единственное условие – объем зашифрованной информации не должен превышать размер файла – хранилища. Для выполнения данного условия, зачастую, программы шифраторы просто заменяют определенные пиксели в изображении.

Как известно, цифровое изображение - это матрица пикселей. Каждый пиксель имеет фиксированную размерность двоичного представления, например, пиксели полутонового представления, кодируются восемью битами. LSB – младший значащий бит, содержит в себе меньше всего информации. Известно также, что человеческий глаз не способен заметить изменения в младших битах, поэтому он используется для встраивания секретной информации.

К сожалению, данный метод подходит не для всех форматов цифрового изображения. Так как, при различных преобразованиях, таких как сжатие или распаковка, не все форматы сохраняют значения младших разрядов. Также, желательно использовать не искусственно созданное изображение, а отсканированную фотографию, так как в таких файлах присутствует множество шумов, в которые легко зашифровать информацию. Также стоит избегать изображения с большим количеством черного и ярких цветов, так как на таких изображениях стегобайты будут характерно выделяться.

Третий рассмотренный метод - метод встраивания информации в аудиозаписи.

При шифровании информации в аудио, также как и с изображениями можно заменять младшие биты, так же можно строить алгоритм шифрования, основываясь на особенностях слуха человека. Человеческое ухо воспринимает сигналы в диапазоне 10 – 20000 Гц, также, изменение фазы сигнала улавливается человеком слабее, чем изменение амплитуды или частоты. Основываясь на этих данных, можно шифровать информацию тремя способами:

1. Незначительная модификация амплитуды отсчетов;
2. Шифрование с помощью модификации разности фаз;
3. Шифрование с помощью изменения задержки эхо – сигнала.

Достоинство данного метода в размере контейнера – он значительно больше, чем при использовании изображения, очевидными недостатками же становятся уловимые человеческим ухом шумы, при встраивании информации.

Последними в данной статье методами, будут методы встраивания информации в видеозаписи.

Данный метод набирает всю большую популярность, так как обмен видеофайлами в современном мире не вызывает никаких подозрений. Существует множество ресурсов(таких как YouTube), на которых видеозаписи хранятся в свободном доступе, что дает большой потенциал для сокрытия в них информации.

Для шифрования информации чаще всего используются форматы MPEG2 и MPEG4. Рассмотрим поподробнее способы внедрения информации в MPEG2:

1) Метод встраивания информации на уровне битовой плоскости.

Этот метод характерен высокой пропускной способностью и небольшой вычислительной сложностью. Существенным недостатком является то, что информация зашифрованная подобным способом может быть легко удалена.

2) Метод встраивания информации на уровне коэффициентов.

Биты скрываемой информации встраиваются в коэффициенты дискретного косинусного преобразования (ДКП). Это позволяет получить энергетический спектр участка изображения.  недостатком данного метода являются искажения, вызванные изменение коэффициентов ДКП, которые могут распространяться во времени и в пространственных областях. Преимущество данного метода в том, что скрытая информация защищена от шумов, фильтров и сжатия.

**Вывод:**

Исходя из всего вышесказанного, можно сделать вывод, что стеганография остается надежным способом сокрытия информации на сегодняшний день. Но у этого способа есть как достоинства, так и множество недостатков, таких как сложность при составлении адекватного текста – контейнера, в случае с текстовыми файлами, либо же очевидное искажение графических файлов, при сокрытии в нем сообщения. Но, несмотря на это, стеганографические методы пользуются популярностью в определенных сферах, связанных с защитой информации.

**Литератур****а**

1. Быков С. Ф. Алгоритм сжатия JPEG с позиции компьютерной стеганографии - Защита информации. Конфидент. — СПб.: 2010
2. Грибунин В.Г., Оков И.Г., Туринцев И.В. Цифровая стеганография. – М.:СОЛОН-Пресс, 2012.