Аскарова Н.Т. Анализ атак и стеганографических методов защиты информации. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVI Междунар. научно-техн. конф. – Пенза: ПДЗ, 2016. – С. 5-12.

УДК 004

АНАЛИЗ АТАК И СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Н.Т. Аскарова

ANALYSIS OF THE ATTACKS AND STEGANOGRAPHIC TECHNIQUES OF INFORMATION SECURITY

N.T. Askarova

Аннотация. Рассмотрены современные методы стеганографического шифрования, виды атак на стеганографические системы и возможные угрозы их безопасности, выявлены достоинства и недостатки стеганографических методов шифрования.

Ключевые слова: стеганография, стеганографический канал, стеганографическая система.

Abstract. In this article the main threats, the attacks to steganographic systems and the modern methods of steganographic encoding were considered, and also merits and demerits of each of them are revealed.

Keywords: steganography, steganographic channel, steganographic system.

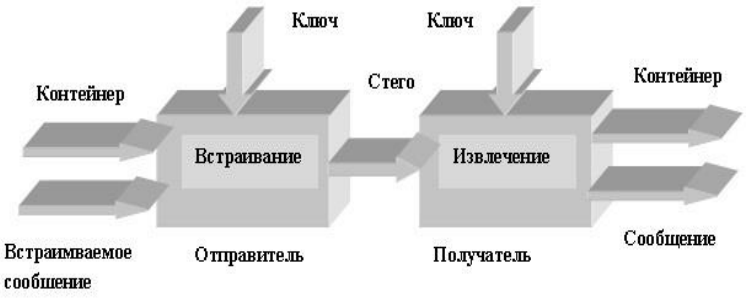
Стеганография – это наука о сокрытии информации методом сохранения в тайне самого факта обмена информацией. Главное отличие стеганографии от криптографии состоит в том, что скрывается не только сообщение, но и информация о передаче сообщения. Также стеганография существенно отличается от криптографии тем, что при стеганографических методах шифрования сообщение встраивается в изображение, аудиозапись или текст, то есть в безобидный объект, который не привлекает внимания злоумышленников.

Наиболее эффективным методом шифрования является совмещение криптографии и стеганографии.

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

Рассмотрим подробнее элементы стеганографической системы.

Контейнер – информация, в которой 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.



Обобщенная модель стегосистемы

В литературе приводятся следующие виды основных угроз безопасности стеганографических систем на современном этапе их развития. Подчеркнем, что во всех вариантах задача противника состоит в том, чтобы отличить стего от пустого контейнера [1].

Обнаружение стеганографического канала. Это самая слабая из угроз безопасности стеганосистем. Она может быть осуществлена пассивным противником. Сама семантика слова «стеганография» требует признать стеганосистему нестойкой, если противник может обнаружить создаваемый ею стеганографический канал. Поэтому о защите от этой угрозы часто говорят как об основной задаче стеганографии. Заметим, однако, что в большинстве работ не уточняется, что понимается под обнаружением стеганографического канала. Здесь имеются две возможности:

- передается последовательность контейнеров, и либо все они пустые, либо часть из них являются стего, созданными с помощью одной и той же стеганосистемы (такой стеганографический канал называется каналом с повторениями). Если не все контейнеры пустые, то противник должен рано или поздно установить этот факт;

- передается один контейнер и противник должен распознать, содержит ли этот контейнер встроенное сообщение (канал без повторений).

Извлечение скрытого сообщения. Противник должен найти скрытое сообщение, содержащееся в данном стего. Существует и более слабый вариант этой угрозы: противник должен получить какую-либо частичную информацию о скрытом сообщении. Эта угроза также может быть осуществлена пассивным противником.

Разрушение скрытого сообщения. Такая угроза существует только со стороны активного противника. В этом случае заинтересованная сторона должна внести в контейнер такие допустимые изменения, чтобы в результате получатель не смог извлечь из него скрытое сообщение (если таковое в нем было).

Подмена скрытого сообщения. Это самая сильная из угроз, осуществляемая только активным противником. Содержащееся в контейнере скрытое сообщение злоумышленник должен заменить другим, выгодным ему сообщением так, чтобы получатель не заподозрил подмену.

Существуют две основные характеристики угроз безопасности стеганографических систем: сила угрозы и сложность осуществления угрозы.

Сила угрозы определяется тем, насколько серьезными могут быть последствия ее осуществления для отправителя и получателя (например, подмена скрытого сообщения – это самая сильная из угроз).

Что же касается сложности осуществления угроз, то здесь ситуация не настолько простая, как это может показаться на первый взгляд. В литературе нередко можно встретить утверждения, что активный противник имеет значительное преимущество в том смысле, что разрушить скрытое сообщение значительно проще, чем обнаружить стеганографический канал. Например, если скрытое сообщение пересылается в младших битах пикселей изображения, то активному противнику достаточно заменять эти биты во всех контейнерах (независимо от того, являются ли они пустыми) на случайные.

Известны следующие основные типы атак на стеганографические системы [2].

Атака с известным стего. Эта самая слабая из всех возможных атак, которую всегда может провести пассивный противник. В случае стеганографического канала без повторений предполагается, что в распоряжении злоумышленника имеется только контейнер, который отправитель передавал получателю. На основе анализа этого контейнера злоумышленник должен осуществить свою угрозу безопасности стеганосистемы (обнаружить, извлечь, разрушить, подменить). Для стеганографического канала с повторениями возможны два варианта этой атаки:

1. Злоумышленник получает некоторую последовательность контейнеров, пересылаемых отправителем получателю. Если среди этих контейнеров имеются стего, то предполагается, что все они созданы с помощью одной и той же стеганосистемы. Если угрозой является обнаружение стеганографического канала, то данная атака очевидным образом сводится к предыдущему случаю (одного контейнера). Для остальных типов угроз ситуация несколько сложнее, но также позволяет перейти при соответст-вующей переформулировке угрозы к случаю одного контейнера.

2. Злоумышленник получает последовательность $C = \{c_1, ..., c_n\}$ контейнеров, пересылаемых отправителем получателю. Кроме того, злоумышленнику известно, что все контейнеры из некоторого подмножества $C_1 \subseteq C$ пустые, а контейнеры из $C_2 \subseteq C$ являются стего. Как и прежде, предполагается, что все стего из C, а также контейнер c_{n+1}, если он не пустой, созданы одной и той же стеганосистемой. Злоумышленник получает также информацию, частичную или полную, о скрытых сообщениях, которые содержатся в стего из множества $C_3 \subseteq C_2$. Далее злоумышленник получает контейнер c_{n+1} и должен на основе его анализа осуществить угрозу безопасности стеганосистемы. Принципиальное отличие от случая 1 в том, что угроза безопасности, какой бы она ни была, относится только к контейнеру c_{n+1}.

Атака с известным контейнером. Злоумышленник получает контейнер, пересылаемый отправителем получателю, и соответствующий ему пустой контейнер. Детерминированный случай тривиален. Более содержателен следующий сценарий. В каждый контейнер перед передачей по каналу связи между отправителем и получателем вносятся небольшие случайные искажения. Злоумышленник знает исходный пустой контейнер и контейнер, передаваемый по каналу связи. Ее основная задача – понять, что содержится в последнем контейнере – случайный шум или скрытое сообщение.

Естественным усилением данной атаки является атака с выбором контейнера, когда злоумышленник имеет возможность выбрать исходный пустой контейнер.

Атака с известным скрытым сообщением. Эта атака возможна только в случае стеганографического канала с повторениями и может быть осуществлена пассивным противником. Предполагается, что злоумышленник знает стего и, быть может, соответствующий пустой контейнер. Кроме того, он каким-то образом узнает скрытое сообщение, встроенное в стего, и использует эту информацию для анализа используемой стеганосистемы (например, пытается определить секретный ключ, чтобы реализовать какие-либо угрозы безопасности стеганосистемы в будущем).

Атака с выбором скрытого сообщения. Аналогична предыдущей, но противник может сам выбирать скрытое сообщение. Разумеется, такую атаку может

провести только активный противник. Возможен, например, следующий сценарий: злоумышленник «подбрасывает» нужное ему сообщение отправителю и, получив стего, пытается определить секретный ключ стеганосистемы.

В перечень рассмотренных в литературе стеганографических методов защиты информации попали: методы сокрытия информации в текстовых файлах, методы шифровки в аудио/видеофайлах, а также методы сокрытия информации в графических файлах [3].

При использовании стеганографических методов защита информации происходит на трех уровнях:

- неизвестен сам факт обмена информацией;
- неизвестен ключ;
- неизвестен алгоритм шифрования информации.

Наиболее распространенным является метод ***встраивания секретной информации в тексты***.

Этот метод делится на два типа:

1. Синтаксическое встраивание скрытой информации.

Сокрытие информации происходит путем изменения количества пробелов, табуляции, изменения межстрочных интервалов, использования невидимых символов, регистров 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.

Эти системы основаны 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 преимущество 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 битов. В одно слово обычно кодируется два бита информации из стегосообщения. Например, слова, состоящие из 5-10 символов, могут 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 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. При этом младший значащий бит (LSB)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 метод – это метод ***встраивания информации в аудиозаписи***.

При встраивании информации в аудио, как и в изображениях можно заменять младшие биты, можно строить алгоритм шифрования, основываясь на особенностях слуха человека (человеческое ухо воспринимает сигналы в диапазоне 10 – 20000 Гц и слабее улавливает изменение фазы сигнала, чем изменение амплитуды или частоты). Основываясь на этих данных, можно шифровать информацию тремя способами:

1. Незначительной модификацией амплитуды отсчетов.
2. С помощью модификации разности фаз.
3. С помощью изменения задержки эхо-сигнала.

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

В качестве последнего рассмотрим ***метод встраивания информации в видеозаписи***.

Данный метод набирает все большую популярность, так как обмен видеофайлами в современном мире не вызывает никаких подозрений. Существует множество ресурсов, на которых видеозаписи хранятся в свободном доступе, что дает большой потенциал для сокрытия в них информации [3].

Существуют следующие способы внедрения информации в видео:

1. Встраивание 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. Встраивание информации на уровне коэффициентов. Биты скрываемой информации встраиваются в коэффициенты дискретного косинусного преобразования (ДКП), позволяющие 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.

Исходя из всего вышесказанного, можно сделать вывод, что, несмотря на разнообразие атак на стеганографические системы, 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 сферах, связанных с защитой информации.

Библиографический список

1. Варновский Н.П., Голубев Е.А., Логачёв О.А. Современные направления стеганографии // Математика и безопасность информационных технологий: материалы конференции МГУ, 28-29 октября 2004. М., 2004. С. 32–65.

2. Johnson N. F., Jajodia S. Steganalysis of images created using current steganography software. Proc. 2nd Intern. Workshop on Inform. Hiding, 1998, LNCS, v. 1525, 273–289.

3. Борисюк Д.Е. Анализ стеганографических методов защиты информации. URL: http://sci-article.ru

Аскарова
Нурсанат Темирбековна
Казахский национальный исследовательский технический университет имени К.И. Сатпаева, г. Алматы, Казахстан,
Люблинский технический университет, г. Люблин, Польша
E-mail: askarova_ns@mail.ru

Askarova N.T.
Kazakh National Research Technical University named after K.I. Satpayev, Almaty, Kazakhstan,
Lublin University of Technology, Lublin, Poland