УДК 003.26

СОВРЕМЕННАЯ КОМПЬЮТЕРНАЯ СТЕГАНОГРАФИЯ В ПРОГРАММИРОВАНИИ

И.В. ИСАКОВ
(*Представлено: канд. физ.-мат. наук, доц. Ю.Ф. ПАСТУХОВ*)

В данной работе рассмотрим и проанализируем основные направления современной компьютерной стеганографии, её обобщенную модель и схему построения.

Стеганография – это наука о скрытой передаче информации, при этом сам факт передачи остается в тайне. Криптография же, осуществляет скрытие информации путём её шифрования. Так же, в отличие от криптографии, стеганография скрывает наличие самого передаваемого сообщения. Данное скрытие осуществляется различными способами, для которых общей чертой является то, что скрываемое сообщение встраивается в некоторый простой, не привлекающий внимание объект. После чего, объект открыто передается адресату. И как мы уже знаем, наличие скрытой связи остается незаметным. Так же, дабы дополнить стеганографию, совместно с ней обычно используют методы криптографии.

В компьютерной стеганографии передаваемые данные встраивают в цифровые, которые как правило имеют аналоговую природу, то беж – речь, видео, изображения, аудиофайлы. В компьютерной стеганографии имеются два основных направления – связанное и не связанное с цифровой обработкой сигнала/ [1]

Направления стеганографии. Современная стеганография — цифровая и компьютерная. Последнюю можно разделить на три больших направления. Первое — это собственно тайнопись, или методы сокрытия одних файлов (которые принято называть сообщением) внутри других («контейнера»). После заполнения сообщением контейнер внешне меняется незаметно и полностью сохраняет свою функциональность. Второе направление изучает методы добавления к сообщению скрытых или стеганографических меток (stegomarks). Это незаметные без специальной обработки метки, идентичные для всех файлов одного человека или устройства. Например, такие стегометки записываются в цифровые фотографии для того, чтобы можно было доказать их авторство. Крэкеры иногда оставляют стегометки в лицензионных ключах. Они зашиты на уровне алгоритма генерации, а потому сохраняются при попытке изменить интерфейс кейгена и выдать его за свой. Третье направление — внедрение в сообщение цифровых отпечатков (digital fingerprints). В отличие от стегометок, эти скрытые знаки уникальны для каждого сообщения. Они служат в основном для защиты интересов правообладателей, позволяя отследить распространение контента. К примеру, многие интернет-магазины внедряют цифровые отпечатки в продаваемые книги и музыкальные композиции. В них кодируется информация о дате продажи и аккаунте купившего (имя, IP-адрес и прочее). Если купленные файлы позже появятся среди торрентов или на файлообменниках, то правообладатели смогут установить распространителя нелегального контента. Для этого будет достаточно считать из контрафактного файла вкрапленный цифровой отпечаток. Использует ли наш любимый онлайновый сервис стегометки? Это легко проверить. Достаточно купить два экземпляра одного и того же произведения с разных аккаунтов и сделать побайтное сравнение файлов. Разница между ними и покажет скрытые метки. Если же файлы скачались идентичные (и их хеши полностью совпадают), то стегометок внутри нет. [2]

Строение стегосистемы. Стегосистема является совокупностью средств и методов, которые используются для формирования скрытого канала передачи данных. Стегосистема выполняет задачу встраивания и выделения сообщений из другой информации. Обобщенная модель стегосистемы представлена на рис.1 Она состоит из множества основных элементов [3]:

Пустой контейнер – контейнер? не содержащий встроенного сообщения; Контейнер – любая информация, предназначенная для сокрытия сообщений;

Стего-контейнер – содержит встроенную информацию;

Встроенное сообщение – собственно само сообщение, которое встраивается в контейнер;

Стегоканал – канал передачи стего-сообщения;

Стегоключ – в зависимости от уровня защиты может быть несколько ключей. Данный ключ предназначен для сокрытия информации;

Прекодер – предназначен для того чтобы преобразовать сообщение? которое необходимо скрыть, к удобному для встраивания в сигнал-контейнер виду;

Стегокодер – устройство, с помощью которого осуществляется вложение сообщения в другие данные, учитывая их модели;

Стегодетектор – определяет наличие стегосообщения;

Рисунок 1. – Обобщенная модель стегосистемы

При построении стегосистемы, должны соблюдаться следующие положения, требования [3]:

– Стегосообщение обязано быть устойчивым к каким-либо искажениям, особенно злонамеренным. При передаче изображение либо другой контейнер может подвергаться всяко-разным трансформациям: увеличиваться или уменьшаться, изменяться может сам формат и т.д. Так же может произойти сжатие, при чём, могут использоваться алгоритмы сжатия, при которых имеет место потеря данных.

– Свойства контейнера должны быть модифицированы таким образом, дабы невозможно было выявить какие-либо изменения при визуальном контроле. Данное требование определяет уровень качества сокрытия встраиваемого сообщения. Стоит отметить, что для обеспечения беспрепятственного прохождения стегосообщения по каналу связи, оно никак не должно привлечь внимание атакующего.

– Для сохранения целостности встраиваемого сообщения необходимо использование кода с исправлением ошибки.

– Для повышения надежности встраиваемое сообщение должно быть продублировано.

– Потенциальный противник должен быть лишен каких-либо технических и иных преимуществ в распознавании или раскрытии содержания тайных сообщений.

– Противник имеет полное представление о стегосистеме и деталях ее реализации. Единственной информацией, которая остается неизвестной потенциальному противнику, является ключ, с помощью которого только его держатель может установить факт присутствия и содержание скрытого сообщения.

– Противник, каким-то образом узнавший о факте существования скрытого сообщения, не должен иметь возможности извлечь подобные сообщения в других данных до тех пор, пока ключ хранится в тайне.

Схема стеганосистемы как системы связи представлена на рисунке 2.

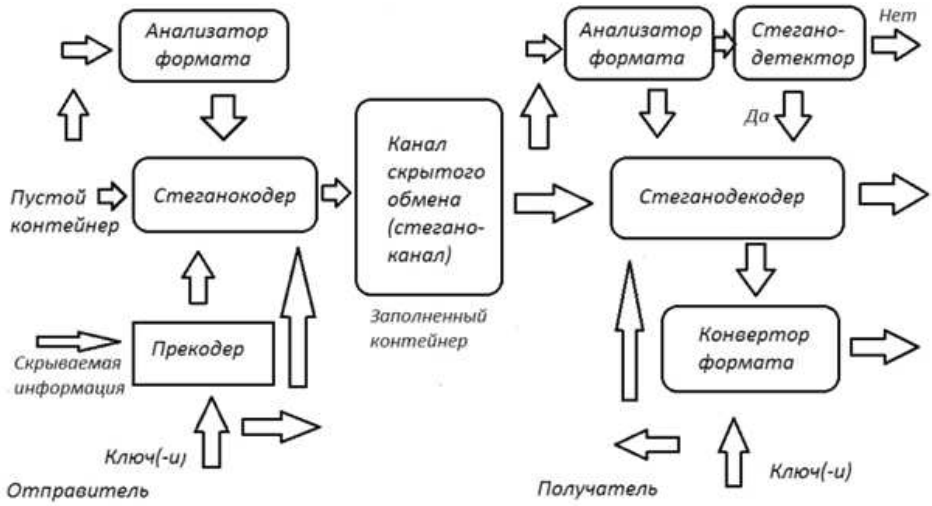

Рисунок 2. – Схема стегосистемы как системы связи

Заключение. Компьютерная стеганография играет важную роль в обеспечении информационной безопасности современного мира, когда существуют такие нерешенные проблемы как защита авторского права, защита прав на личную тайну, организация электронной торговли, компьютерная пре-

ступность и кибертерроризм. Стеганография может обеспечивать помехоустойчивую аутентификацию мультимедийной информации, контроль целостности данных, защиту прав собственника мультимедийной информации, отслеживание распространения информации. Основная проблема современной цифровой стеганографии – отсутствие стандартов. При наличии достаточного числа известных алгоритмов, отсутствует организованная практика их применения. Надеюсь, что в ближайшие годы в результате инициатив молодых специалистов определится в каком-то виде стандарт стеганографических средств защиты информации.

ЛИТЕРАТУРА

1. Садов, В.С. Компьютерная стеганография (Конспект лекций)/В.С. Садов – Минск: БГУ, 2010. – 211 с.
2. Шнайер, Б. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер – СПб.: Питер, 2003. – 368 с.
3. Грибунин, В.Г. Цифровая стеганография/ В.Г. Грибунин – Москва: «Академия», 2009. – 265 с.