http://neerc.ifmo.ru/wiki/index.php?title=Слово_Туэ-Морса
2. e-maxx [Электронный ресурс]. – Электронные данные. – Режим доступа: http://e-maxx.ru/algo/string_hashes

СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Губский М. Д.

Стройникова Е. Д. – ассистент кафедры информатики

Во все времена ценность информации была высока. На протяжении столетий люди использовали всевозможные приемы защиты важных данных от несанкционированного доступа, всякий раз придумывая все более сложные и надежные. Как правило, это были криптографические методы. Но порой лишь зашифровать необходимые сведения являлось недостаточным. Для усиления защиты использовались методы сокрытия информации — стеганографические методы.

На сегодняшний день существует множество способов сокрытия данных. Одним из простых в реализации, но не таким простым в обнаружении, является стеганография.

Стеганография (греч. тайнопись) — наука, изучающая передачу и хранение информации при сокрытии самого факта ее существования. Уже в IV в. до н. э. использовали стеганографию, чтобы передавать важные сообщения. Так, например, наносилось необходимое сообщение на обритую голову раба. Когда волосы отрастали, он отправлялся к адресату, который, сбрив голову, считывал сообщение.

За время своего существования стеганография претерпела множество изменений и дополнений. На современном этапе сформировалось три направления стеганографии: классическая, компьютерная, цифровая.

Классическая стеганография — исторически сложившиеся методы сокрытия сведений, которые применяются в повседневной «реальной» жизни, другими словами, некомпьютерные методы. Например, по одной из версий древние шумеры наносили сообщения на глиняные дощечки, после покрывали их слоем глины и вновь наносили надпись, но уже не секретную. Также можно вспомнить запись сообщений на боковой стороне колоды карт, «жаргонные шифры», акростихи и т. д.

Компьютерная стеганография, как видно из названия, включает в себя методы, основанные на особенностях конкретной платформы компьютеров, а также свойствах компьютерных форматов данных. Примерами компьютерных стеганографических методов являются следующие:

- Метод с использованием регистра букв. Его суть заключается в том, что каждый символ секретного сообщения переводится в байт-код. Затем у каждого символа скрывающего текста, которому соответствует единица сообщения, следует поменять регистр. Таким образом, можно зашифровать максимум N/8 символов, где N — количество символов в скрывающем тексте.
- Метод, использующий специфику файловых систем. Как известно, операционные системы для хранения файлов выделяют целое число блоков (для удобства адресации). Соответственно, для хранения маленьких файлов выделяется лишняя память, в которой как раз можно хранить необходимую информацию.
- Использование зарезервированных полей форматов данных также является отличным методом сокрытия сведений. Метод полагается на то, что большинство мультимедийных форматов имеют поля расширения, не использующиеся программой, как правило, они заполнены нулевой информацией.

На сегодняшний день самым важным и наиболее используемым направлением является цифровая стеганография. Это направление характеризуется тем, что необходимая информация внедряется и скрывается в цифровые объекты. К сожалению, цифровая стеганография накладывает некоторые обязательства, такие как сохранение целостности и аутентичности файла, поэтому обычно в качестве контейнеров (хранилищ данных) используют медиафайлы. Существуют следующие алгоритмы встраивания скрываемой информации:

- работающие с цифровым сигналом напрямую (метод LSB);
- внедрение скрытой информации (наложение секретного изображения, аудиофайла, текста поверх оригинала; часто используется для внедрения цифровых водяных знаков);
- использование форматов файлов (к примеру, запись в метаданные).

Одним из самых известных алгоритмов встраивания является метод LSB (Least Significant Bit — англ. наименьший значащий бит). Он основан на замене последних, незначащих бит в контейнере (графическом, аудио, видеофайле) на биты секретного сообщения. Метод опирается на низкий порог чувствительности человеческих органов. Например, изменение в 8-битном изображении двух последних бит приводит к изменению в цвете максимум на 3 бита, такие градации не отображают многие программы (считая их несущественными), не говоря уже о человеческом глазе.

В общем случае система маскирования имеет следующий вид (рис. 1):

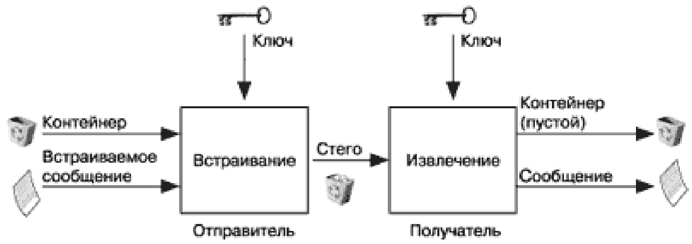

Рис. 1 — Процесс сокрытия данных с помощью цифровой стеганографии

Пояснения к рис. 1:

- Контейнер — любая побочная информация (аудио, видео, изображение), служащая для сокрытия секретных сообщений.
- Встраиваемое сообщение — секретные данные, нуждающиеся в сокрытии.
- Встраивание — внедрение сообщения в контейнер, происходит на компьютере с использованием одного из методов стеганографии и ключа.
- Стего — стеганографический канал, канал передачи внедренного сообщения.
- Извлечение — получение секретного сообщения с использованием ключа.
- Ключ — сведения, необходимые для сокрытия/получения информации. Ключи бывают секретные и открытые. Системы с секретным ключом использует его как для встраивания, так и для извлечения. Системы с открытым ключом — только для встраивания, для извлечения используется независимый ключ.

В ходе исследования была произведена оценка устойчивости метода LSB с использованием изображений на языке Python. Процесс внедрения производился приведенным выше способом (см. рис. 1). В качестве контейнера использовалось изображение формата PNG. Для примера секретным сообщением было выбрано «success_1». Вмонтирование сведений производилось посредством резервирования 2-х последних бит каждого цвета, из которых состоит пиксель изображения в системе RGB. Для работы с изображениями и их трансформацией использовался модуль PIL языка Python. Анализ производился по двум параметрам: незаметность изменений контейнера при добавлении данных и валидность извлеченного сообщения. Примеры работы программы в зависимости от вида трансформации приведены в табл. 1.

Таблица 1. Оценка устойчивости LSB в зависимости от метода трансформации контейнера

Вид трансформации		Без трансформации	EXTENT	AFFINE	PERSPECTIVE
Ввод		success_1			
Вывод	1	success_1	ÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿ	ÿÿÿÿÿÿÿÿÿ
	2		ÿÿÿü8Àõý@	ÝXØÙ\Ü×Ìÿÿ	ÝÇqÇqÇ
	3		qV6Ï_?ÿÿÿ	ß}÷ ß}÷ ß}÷	ÿÿÿýÇqÇ
Видимость		—	—	—	—

Пояснения к табл. 1:

- EXTENT — извлекает область и помещает в новое изображение с данным размером (использовался как resize);
- AFFINE — аффинное преобразование;
- PERSPECTIVE — перспективное преобразование.

Полученные данные показали, что невооруженным глазом определить наличие скрытого сообщения невозможно. Однако быть уверенным, что сообщение будет доставлено в целости и сохранности, нельзя. Таким образом, метод LSB является не устойчивым ко всякого рода трансформациям контейнера, т. е. метод хорош лишь при использовании статических контейнеров (не подверженных изменениям).

В заключение хотелось бы отметить, что стеганография не является должной заменой криптографии и полагаться только на нее не стоит. Но в сочетании с криптографическими методами стеганография становится еще одним рубежом защиты вашей бесценной информации.

Список использованных источников:

1. Грибунин, В. Г. Цифровая стеганография / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев. – М. : СОЛОН-Пресс, 2002. — 272 с.
2. Рябко, Б. Я. Основы современной криптографии и стеганографии / Б. Я. Рябко, А. Н. Фионов. — 2-е изд. — М. : Горячая линия — Телеком, 2013. — 232 с.
3. CitForum [Электронный ресурс]. — Режим доступа : http://citforum.ru.