М. О. Жмакин

СТЕГАНОГРАФИЯ И ПЕРСПЕКТИВЫ ЕЕ ПРИМЕНЕНИЯ В ЗАЩИТЕ ПЕЧАТНЫХ ДОКУМЕНТОВ

Надежная защита информации от несанкционированного доступа является древнейшей и в полной мере не решенной в настоящее время задачей. Методы сокрытия секретных сообщений известны с давних времен. Данная сфера человеческой деятельности получила название **стеганография.** Это слово происходит от греческих слов steganos (секрет, тайна) и graphy (запись) и, таким образом, означает буквально «тайнопись», хотя методы стеганографии появились, вероятно, раньше, чем появилась сама письменность (первоначально использовались условные знаки и обозначения).

Как известно, цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Стеганография имеет другую задачу, и ее цель — скрыть сам факт существования секретного сообщения. При этом оба способа могут быть объединены и использованы для повышения эффективности защиты информации (например, для передачи криптографических ключей).

В современном понимании стеганографическая система (или просто стегосистема) — это совокупность средств и методов, которые используются для формирования скрытого канала передачи информации (Рис. 1).

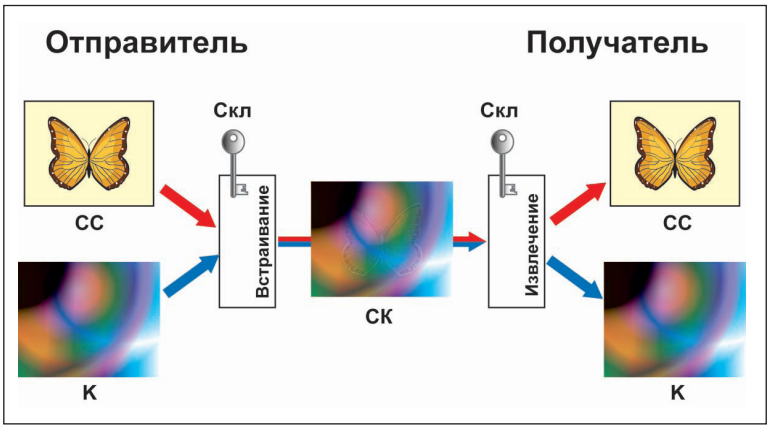

Рис. 1. Стеганографическая система

Общий процесс стеганографии выражается простой формулой:

К + СС + СКл = СК,

где:

- *контейнер* **(К)** — любая информация, предназначенная для встраивания тайных сообщений;
- *скрываемое (встраиваемое) сообщение* **(СС)** — тайное сообщение, встраиваемое в контейнер;
- *стегоключ* **(СКл)** — секретный ключ, необходимый для скрытия (шифрования) информации. В зависимости от количества уровней защиты (например, встраивание предварительно зашифрованного сообщения) в стегосистеме может быть один или несколько стегоключей;
- *стегоконтейнер* **(СК)** — контейнер, содержащий встроенное сообщение;
- *стеганографический канал* (стегоканал) — канал скрытой передачи информации.

Чтобы не вызывать подозрений у стороннего наблюдателя, передаваемый стегоконтейнер практически ничем не должен отличаться от исходного контейнера. Но этого мало. Чтобы стегосистема была надежной, при ее построении необходимо исходить из предположения, что противник имеет полное представление о применяемой стеганографической системе и деталях ее реализации. Единственной неизвестной ему величиной является стегоключ.

Исходя из этого предположения, стегосистема должна быть сконструирована таким образом, чтобы только обладатель стегоключа имел возможность выделить из стегоконтейнера встроенное сообщение и, главное, чтобы только обладатель стегоключа имел возможность установить факт присутствия скрытого сообщения.

В настоящее время стеганографию можно условно разделить на три раздела:

1. Классическая стеганография, которая включает в себя все «некомпьютерные методы»;

2. Компьютерная стеганография — направление классической стеганографии, основанное на особенностях компьютерной платформы и использовании специальных свойств компьютерных форматов данных;

3. Цифровая стеганография — направление классической стеганографии, основанное на сокрытии или внедрении дополнительной информации в цифровые объекты, что вызывает некоторые искажения этих объектов. Чаще всего в этих целях используется избыточность аудио- и визуальной информации.

Коротко остановимся на компьютерной и цифровой стеганографии.

Компьютерная (и как частный случай — цифровая) стеганография — это раздел стеганографии, который занимается вопросами реализации стегосистем с использованием компьютерной техники, путем внедрения скрываемой информации в цифровые объекты, с некоторыми искажениями этих объектов.

Поскольку цифровая информация обычно передается в виде файлов, в компьютерной стегосистеме используются понятия *файл-сообщение* и *файл-контейнер*.

Файл-сообщение содержит скрываемую информацию, *файл-контейнер* может быть использован для сокрытия в нем сообщения. Под ключом понимается секретный элемент, который определяет порядок занесения сообщения в контейнер. Для того чтобы посторонние не заподозрили факт передачи сообщения, файл-сообщение особым образом (при помощи стегоключа) «смешивают» с файлом-контейнером. При этом, как и в «классической» стеганографии, файл-контейнер должен выглядеть вполне безобидно, а подмешивание секретной информации не должно изменять его основных свойств. В большинстве случаев в качестве контейнеров используют мультимедиа-файлы: изображения, видео, аудио, текстуры 3D-объектов. Внешние проявления в этих файлах, связанные с внесением искажений, т. е. с записью скрываемого сообщения, находятся ниже порога чувствительности среднестатистического человека. Кроме того, в оцифрованных объектах, изначально имеющих аналоговую природу, всегда присутствует шум квантования. Далее, при воспроизведении

этих объектов появляются дополнительный аналоговый шум и нелинейные искажения аппаратуры, что способствует большей незаметности сокрытой информации.

Основные принципы современной компьютерной стеганографии можно свести к следующему:

- методы скрытия должны обеспечивать аутентичность и целостность файла;
- предполагается, что противнику полностью известны возможные стеганографические методы;
- безопасность методов основывается на сохранении стеганографическим преобразованием основных свойств открыто передаваемого файла при внесении в него секретного сообщения и некоторой неизвестной противнику информации — ключа;
- даже если факт скрытия сообщения стал известен противнику через сообщника, извлечение самого секретного сообщения должно представлять сложную вычислительную задачу.

Анализ информационных источников в сети Интернет позволяет сделать вывод, что в настоящее время компьютерные стеганографические системы используются для решения таких задач, как защита конфиденциальной информации от несанкционированного доступа, преодоление систем мониторинга и управления сетевыми ресурсами, камуфлирование программного обеспечения и защита авторского права на некоторые виды интеллектуальной собственности.

Перейдем к классической, не компьютерной стеганографии. В этот раздел попадают весьма разнообразные и изощренные методы сокрытия информации, большинство из которых, несомненно, имеет исторический интерес. Но в данном случае нас будет интересовать применение стегосистем в сокрытии информации на печатном оттиске. Идея передачи скрытого сообщения с использованием в качестве стегоконтейнера печатного или рукописного документа далеко не нова. Сразу же вспоминается исторический факт, как В. И. Ленин, находясь в тюремном заключении, писал свои труды молоком, используя в качестве стегоконтейнера межстрочное пространство подручных книг, и отправлял рукописи на свободу, обходя строгий контроль со стороны надзирателей. Как альтернатива, использовать стеганографию в печатном или рукописном документе можно также и для идентификации и/или защиты от подделки самого документа. В этом случае скрываемое сообщение может быть весьма коротким, например идентификационным номером, что осложняет обнаружение наличия скрытой записи. В любом случае, стегосистема должна быть построена таким образом, чтобы при копировании или попытке подделать защищаемый документ скрытое сообщение либо уничтожалось, либо искажалось. Конечно же, все принципы, которые были отмечены ранее для компьютерной стеганографии, действуют и сейчас.

На сегодняшний день существует масса различных стеганографических систем, позволяющих записывать скрываемое сообщение в элементы дизайна печатного документа, выводить на печать, а впоследствии считывать с оттиска «закодированную» информацию. Как правило, запись осуществляется внесением дополнительных или искажением уже существующих графических элементов макета документа, т. е. в общем случае встраиваемое сообщение записывается тем или иным искажением визуального графического изображения, наносимого печатным способом на защищаемый документ. Одним из наиболее тривиальных методов является нанесение печатным способом на продукцию некоторой совокупности распределенных по определенному алгоритму маркирующих элементов. Печать может наноситься как на живописное поле, т. е. непосредственно на изображение, запечатываемое на защищаемую продукцию, так и на незапечатываемую (чистую) область. Как правило, маркирующие элементы наносятся желтой краской, которая в полиграфии считается «слепой», чтобы уменьшить визуальное восприятие этих элементов. При считывании визуальное изображение с комбинацией маркирующих элементов сканируется, выделяется графическими фильтрами и прочитывается с применением стегоключа.

Одним из серьезных недостатков применения существующих методов стеганографии в печати можно назвать то, что при записи скрываемого сообщения искажение оригинального изображения носит выраженный искусственный характер. Это снижает эффективность системы.

Было выдвинуто предположение, что искажения, возникающие на графических элементах отпечатанного оттиска и обусловленные технологическими особенностями вида печати, могут скрыть факт наличия некоторого дополнительного вмешательства в графический дизайн печатного документа. Искажения графической информации на оттисках возникают при любом виде печати, при этом они имеют свой, особенный для каждого вида, характер. Эти искажения могут быть вызваны следующими причинами: техническое состояние машины, параметры печати, вид носителя (в общем случае бумажное полотно), сорт краски, состояние окружающей среды в печатном цехе, квалификация персонала и т. д. Поскольку учесть все факторы, влияющие на качество печати, практически невозможно, а также трудно однозначно определить характер и силу этого влияния, примем воздействие совокупности этих факторов на оригинальное изображение как «зашумление» полезного сигнала. Таким образом, изображение на оттиске имеет характерное зашумление, обусловленное искажением геометрии растровой точки, неравномерным растеканием краски по поверхности листа бумаги и другими технологическими особенностями вида печати. Данное «зашумление» проявляется в так называемом размытии контура графических элементов композиции и в неравномерной заливке плашечных областей изображения. Эти явления в визуальном образе отпечатанного изображения могут быть использованы для сокрытия факта искусственного вмешательства в графический дизайн документа. Т. е. на этапе подготовки к печати в дизайн живописного поля документа вносятся изменения, которые в дальнейшем, при печати, камуфлируются под фрагменты шума, что нейтрализует существенный недостаток стеганографических систем, применяемых для сокрытия информации в оттисках печатных документов.

СПИСОК ЛИТЕРАТУРЫ:

1. *Овсянников В., Чеховский С.* Скрытая утечка информации // Информационная безопасность офиса. Выпуск 1: Технические средства защиты информации. Киев, 2003.
2. *Барсуков В. С., Романцов А. П.* Компьютерная стеганография вчера, сегодня, завтра. Технологии информационной безопасности 21 века // Специальная техника. 1998. N.4–5. URL: http://st.ess.ru/.
3. URL: www.cypher.net.
4. URL: www.demcom.com/english/steganos.