Введение

Развитие средств цифровой обработки, хранения, защиты и передачи информации привело к появлению возможностей массового использования технологий скрытия информации. Для соблюдения авторского права в изображения, видео и аудиозаписи добавляют водяные знаки. В передаваемые данные внедряют специальные метки для помехоустойчивой аутентификации и отслеживания распространения информации по инфокоммуникационным системам. Защита программного обеспечения также предполагает использование методов скрытия уникальных меток в коде.

В первой главе основное внимание уделено методам скрытия данных в различных цифровых объектах: текстах, изображениях, видео- и аудиофайлах. Акцент сделан на перспективных методах — скрытии данных с использованием корректирующих кодов и сетевой стеганографии. Отдельно изложены особенности обеспечения скрытности радиотехнических систем и наиболее распространенные сигналы, которые могут применяться для этих целей.

Вторая глава посвящена апробации перспективных методов на основе корректирующих кодов и сетевой стеганографии. Приведены примеры вкрапления искусственных ошибок при передаче данных по телекоммуникационной системе с использованием моделей в среде Matlab. Они позволяют исследовать эффективность применения корректирующих кодов и подобрать наиболее подходящий для скрытия данных без существенного ухудшения процесса передачи и для их искажения. Также ряд демонстрационных моделей показывает возможность обнаружения фактов передачи стегоданных по сетям с использованием стека протоколов TCP/IP.

1 Основные понятия и методы скрытия передаваемой информации как одного из способов защиты от несанкционированного доступа

Защита информации от несанкционированного доступа является одной из актуальных задач на протяжении длительного времени. Исторически сложились два основных направления решения этой задачи, существующие в настоящее время: криптография и стеганография. Целью криптографии является скрытие содержимого сообщений путем их шифрования. В отличие от шифрования стеганография скрывает сам факт существования тайного сообщения. Скрытие информации осуществляется самыми различными методами (рис. 1). Общей чертой этих методов является то, что скрываемое сообщение встраивается в не привлекающий внимание объект, которым может являться файл в формате, допускающем искажения или содержащий избыточные служебные поля, заголовок сетевого пакета или их последовательность и т. д. Затем этот объект открыто передается приемной стороне.

В прошлом веке широко использовались так называемые симпатические чернила, невидимые при обычных условиях. Скрытое сообщение размещали в определенные буквы словосочетаний, передавали при помощи внесения в текст незначительных стилистических, орфографических или пунктуационных погрешностей. С широким распространением фотографии появилась технология микрофотоснимков, успешно применяемая Германией во время мировых войн. Скрытие информации перечисленными методами возможно лишь благодаря тому, что противнику неизвестен метод скрытия. Между тем, еще в 1883 году Керкгоффс писал о том, что система защиты информации должна обеспечивать свои функции даже при полной информированности противника о ее структуре и алгоритмах функционирования. Вся секретность системы защиты передаваемых сведений

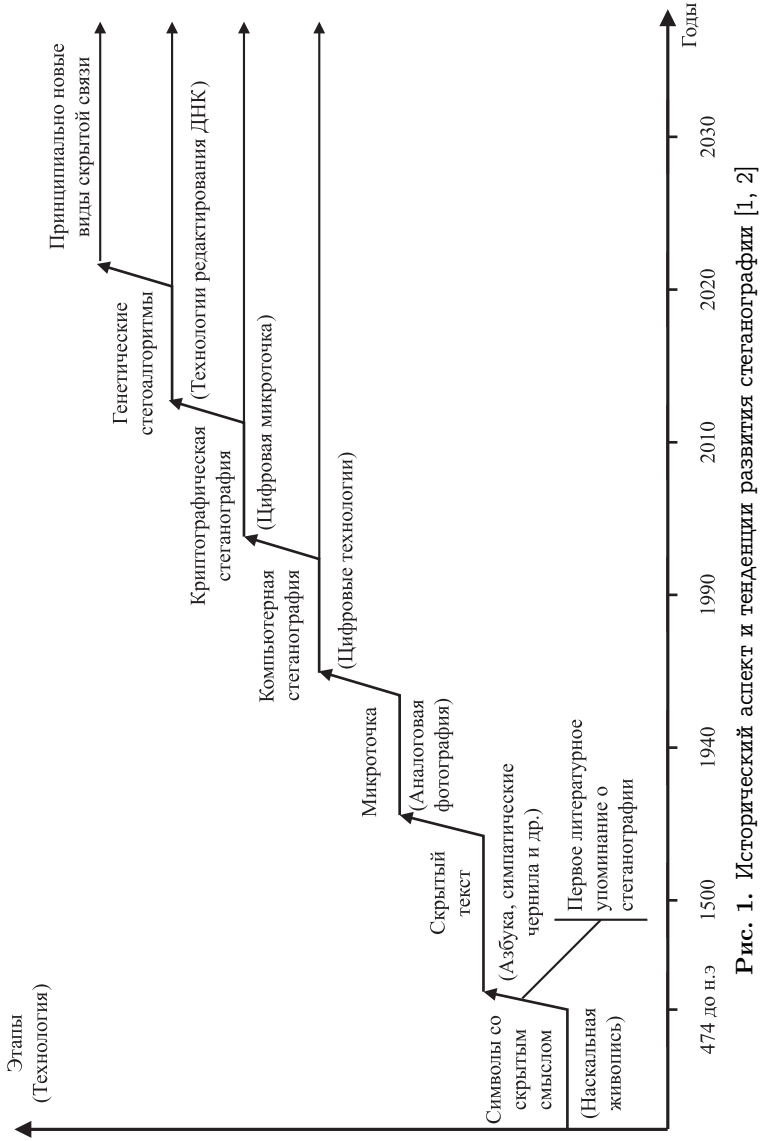

Рис. 1. Исторический аспект и тенденции развития стеганографии [1, 2]

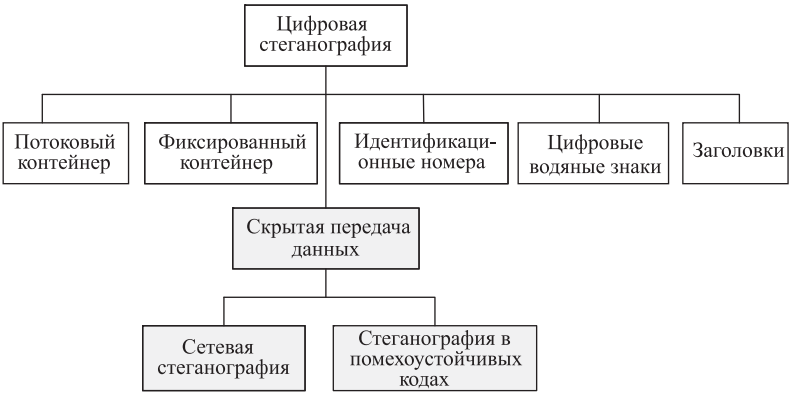

Рис. 2. Классификация областей применения цифровой стеганографии

основана на ключе, т. е. на предварительно (как правило) разделенном между адресатами фрагменте информации.

Расширение функционала и производительности средств вычислительной техники в последние десятилетия привело к развитию компьютерной стеганографии. Появилось много новых областей ее применения. Сообщения встраивают в цифровые данные, как правило, имеющие аналоговую природу: речь, аудиозаписи, изображения, видео. Известны также предложения по встраиванию информации в текстовые файлы и в исполняемые файлы программ. Развиваются направления, связанные с активным использованием протоколов передачи данных и внедрением стегоданных в заголовки пакетов на различных уровнях модели взаимодействия открытых систем OSI, в том числе с применением потерь пакетов и внесением дополнительных ошибок в процесс передачи информации. Этим направлениям будет уделено особое внимание в данном учебном пособии.

Существуют два основных направления в компьютерной стеганографии: связанное с цифровой обработкой сигналов и не связанное. В последнем случае сообщения могут быть встроены в заголовки файлов, заголовки пакетов данных. Это направление имеет ограниченное применение в связи с относительной легкостью вскрытия и/или уничтожения скрытой информации. Большинство текущих исследований в области стеганографии связаны с цифровой обработкой сигналов. Это позволяет гово-

рить о цифровой стеганографии. Можно выделить две причины популярности исследований в области стеганографии в настоящее время: ограничение на использование криптосредств в ряде стран мира и появление проблемы защиты авторских прав на информацию, представленную в цифровом виде, в том числе и сети Интернет. На рис. 2 представлена классификация областей применения цифровой стеганографии.

1.1. Основные понятия и определения стеганографии

Стеганографическая система (*стегосистема*) — объединение методов и средств, используемых для создания скрытого канала передачи информации. При построении такой системы условились о том, что:

1) противник представляет работу стеганографической системы. Неизвестным для противника является ключ, с помощью которого можно узнать о факте существования и содержании тайного сообщения;

2) при обнаружении противником наличия скрытого сообщения он не должен суметь извлечь сообщение до тех пор, пока не будет владеть ключом;

3) противник не имеет технических и прочих преимуществ.

Сообщение (*стегоданные*) — термин, используемый для общего названия передаваемой скрытой информации.

Контейнер — так называется любая информация, используемая для скрытия тайного сообщения. *Пустой контейнер* — контейнер, не содержащий секретного послания.

Заполненный контейнер (*стегоконтейнер*) — контейнер, содержащий секретное послание.

Стеганографический канал (*стегоканал*) — канал передачи стегоконтейнера.

Ключ (*стегоключ*) — секретный ключ, нужный для скрытия стегоконтейнера. Ключи в стегосистемах бывают двух типов: закрытые (секретные) и открытые. Если стегосистема использует закрытый ключ, то он должен быть или создан до начала обмена сообщениями, или передан по защищенному каналу. Стегосистема, использующая открытый ключ, должна быть устроена

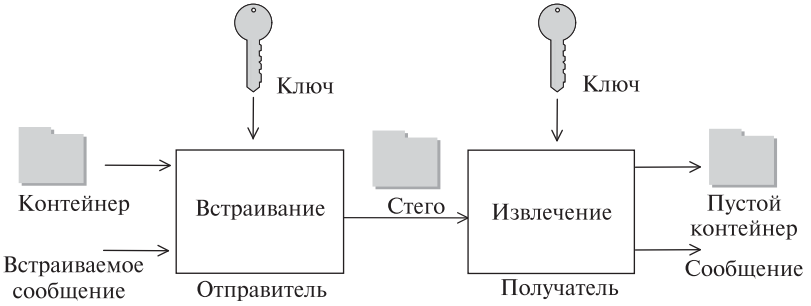

Рис. 3. Обобщенная модель стегосистемы

таким образом, чтобы было невозможно получить из него закрытый ключ. В этом случае открытый ключ можно передавать по незащищённому каналу.

Цифровой водяной знак (ЦВЗ) — специальная метка, внедряемая в цифровой объект (изображение, текст, речь и т. д.) для контроля за его использованием.

Для описания стеганографических систем используют стеганографические модели (рис. 3). Общий случай стеганографической модели был предложен Симмонсом, который назвал ее «проблема заключенных». Ее суть состоит в том, что есть человек на свободе (Алиса), в заключении (Боб) и охранник (Ева). Алиса хочет передавать сообщения Бобу без вмешательства охранника. В этой модели сделаны некоторые допущения: предполагается, что перед заключением Алиса и Боб договариваются о кодовом символе, который отделит одну часть текста письма от другой, в которой скрыто сообщение. Ева же имеет право читать и изменять сообщения.

Кристианом Кашеном была предложена стеганографическая модель под названием «модель стегосистемы с секретным ключом» [3]. На рис. 4 показан принцип работы этой стегосистемы.

Алиса и Боб являются пользователями системы. Алиса хочет отправить сообщение со скрытым смыслом по общественному каналу Бобу так, чтобы присутствие скрытой информации осталось незамеченным для третьей стороны, противника Евы, которая имеет идеальный доступ только для чтения открытого канала.

Переключатель S определяет два возможных состояния Алисы:

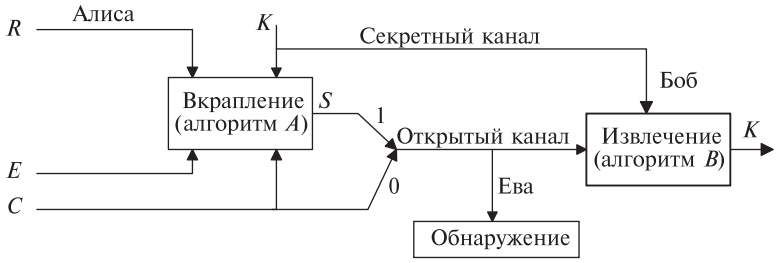

Рис. 4. Модель стегосистемы с секретным ключом

1) *пассивное* состояние (переключатель в позиции 0) — Алиса отправляет только пустые контейнеры C Бобу по открытому каналу передачи данных. Ева имеет возможность просматривать пустые контейнеры C;

2) *активное* состояние (переключатель в позиции 1) — Алиса отправляет стегосообщение E, которое она вкрапила в пустой контейнер C, используя алгоритм A. Имея на входе контейнер C (получаемый случайным источником пустых контейнеров R), ключ K и сообщение E, алгоритм A выдает на выходе стегоконтейнер S. Стегоконтейнер отправляется Бобу по открытому каналу. Противник Ева и получатель принимают S. Используя алгоритм извлечения B, Боб с помощью ключа K извлекает сообщение E'' из S в надежде, что он получил искомое стегосообщение $E = E''$ от Алисы.

У Боба имеется «оракул», с помощью которого он определяет, активна Алиса или пассивна. Термин «оракул» использует сам К. Кашен: «Это серьезное допущение, обозначим его как одно из основных свойств безопасности стегосистемы». Не принимая данное допущение, мы не ухудшим качество системы. Действительно, если Боб попытается извлечь сообщение из контейнера, когда Алиса пассивна, он получит только «мусор». Боб извлекает стегосообщение, когда знает, что Алиса активна, в противном случае он не использует алгоритм извлечения.

Задача Евы определить, когда Алиса передавала пустой контейнер, а когда стегоконтейнер. Обозначим сообщение в канале через M. Если Алиса активна, то $M = S$ (стегоконтейнер), а если пассивна, то $M = C$ (пустой контейнер).

Определим распределения $P_C(y)$ и $P_S(y)$ соответственно как вероятность появления пустого контейнера $y \in C$, если переда-

вался пустой контейнер, и вероятность появления стегоконтейнера $y \in S$, если передавался стегоконтейнер.

Допустим, что P_C и P_S известны Еве. Это напоминает предположение о неограниченных вычислительных ресурсах, которыми обладает противник, при определении Шенноном совершенной криптосистемы в [4]:

$$D(P_{X1} \parallel P_{X2}) = \sum_{x \in X} P_{X1}(x) \log_2 \frac{P_{X1}(x)}{P_{X2}(x)}. \qquad (1)$$

Введем множество $\{\hat{\mathbb{R}} = \mathbb{R} \cup \{\infty\}\}$. Величину $D(P_{X1} \parallel P_{X2})$, заданную формулой (1), называют относительной энтропией из множества X в множество $\hat{\mathbb{R}}$, если определить $0 \log_2 \frac{0}{0} = 0$; $T \log_2 \frac{T}{0} = \infty$. Если хотя бы одно слагаемое в формуле (1) равно ∞, то $D(P_{X1} \parallel P_{X2}) = \infty$. Относительная энтропия не является симметричной величиной, иначе говоря,

$$D(P_C \parallel P_S) \neq D(P_S \parallel P_C).$$

Система называется *совершенной* (от пассивного противника), если относительная энтропия между P_C и P_S равна нулю, т. е. если

$$D(P_C \parallel P_S) = 0.$$

Система называется ε-секретной (от пассивного противника), если

$$|D(P_C \parallel P_S)| \leqslant \varepsilon.$$

Если система совершенная, то, получая на вход контейнер, невозможно с вероятностью, отличной от 0,5, определить, принадлежит ли он к стегоконтейнеру или к пустому контейнеру.

Модель трех каналов. Описание модели трех каналов приведено в [5]. В данной модели выступают пять сторон: Алиса, Боб, Алена, Борис и Иванов. Одна из задач Иванова — определить, какая пара использует стеганографию при передаче сообщения: Алиса и Боб или Алена и Борис.

Алена и Борис передают друг другу контейнеры, не содержащие стегосообщения (пустые контейнеры) (рис. 5). Для этого Алена использует помехоустойчивый код. Перед отправкой информационный вектор подается на кодер A, который выдает на