АНАЛИЗ СТЕГАНОГРАФИЧЕСКИХ МЕТОДОВ

Серкевич Д. С., Герман Ю. О.
Кафедра защиты информации,
кафедра информационных технологий автоматизированных систем,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: sdasha695@gmail.com, jgerman@bsuir.by

В данной работе проведена классификация методов стеганографии для изображений, а также проанализированы их сильные и слабые стороны. Представлена актуальность развития методов стеганографии в сфере кибербезопасности. Понимание принципов функционирования стеганографических методов и их практического применения способствует построению эффективных систем защиты данных от несанкционированного доступа и сохранию конфиденциальности личной информации.

Введение

С ростом распространенности кибератак потребность в безопасных методах передачи информации стала первостепенной. Основная цель стеганографии – скрыть сам факт передачи сообщения, в отличие от криптографии, которая шифрует содержание, но не скрывает саму передачу.

Стеганография в изображениях стала более популярной в последние годы, чем другие виды стеганографии, возможно из-за большого потока изображений в электронном виде, доступного с появлением цифровых камер и высокоскоростной интернет-передачи. Поэтому она играет важную роль в обеспечении информационной безопасности, защите авторских прав и передачи конфиденциальных данных [1].

I. Стеганографическая система

Стеганография – это метод организации связи (передачи сообщений), при котором скрывается само наличие связи.

Стеганографическая система (см. рис. 1) в общем виде состоит из двух компонентов: вставки и извлечения сообщения.

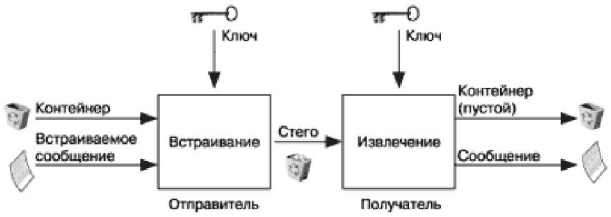

Рис. 1 – Стеганографическая система

Процесс обработки стеганографического сообщения включает следующие объекты:

- сообщение – данные любого типа;
- контейнер – любая информация, пригодная для сокрытия в ней сообщений;
- стегоконтейнер – контейнер, содержащий скрытое сообщение;
- ключ (стегоключ) – секретный ключ, необходимый для шифрования (расшифровки) сообщения с целью усиления защиты.

По аналогии с криптографией, по типу стегоключа стегосистемы можно подразделить на два типа:

1. с секретным ключом;
2. с открытым ключом [2].

II. Методы для временной области

1. *Псевдослучайные перестановки.* Метод вставляет биты сообщения с изменением порядка их появления в сообщении на основе генератора псевдослучайных чисел. Это делает внедрение менее предсказуемым и затрудняет обнаружение скрытых данных.
   Преимущества:
   - метод вставляет биты сообщения, изменяя порядок их следования, что усложняет процесс обнаружения и расшифровки информации;
   - биты скрываемого сообщения равномерно распределены по всему контейнеру.

   Недостатки:
   - бит сообщения, вставленный случайным образом в младший бит контейнера, может быть поврежден;
   - требуется синхронизация ключей между отправителем и получателем [3].
2. *Метод с использованием патчей.* Этот метод является статистическим кодированием информации путем изменения некоторых статистических свойств контейнера и использует проверку гипотез при извлечении сообщения. Секретный ключ применяется к случайно выбранному подмножеству пикселов из изображения, затем подмножество разделяется по двум патчам – A и B.
   Преимущества:
   - устойчивость к атакам;
   - гибкость маскировки;
   - сообщение распределено по всему изображению.

   Недостатки метода:
   - сложность реализации;
   - ограниченная емкость, в один патч инкапсулируется только один бит;

– зависимость от качества сегментации.

3. *Метод расширения спектра.*Модификация метода расширения спектра заключается в изменении базисной функции, которая является произведением гармонического сигнала на псевдослучайную последовательность.Частотная характеристика сообщения обладает гораздо меньшей энергией, чем энергия контейнера.

   Преимущества:
   - высокая устойчивость к шуму и атакам;
   - низкая вероятность обнаружения;
   - применимость к различным типам носителей.

   Недостатки:
   - сложность реализации;
   - низкая емкость;
   - зависимость от качества генерации псевдослучайной последовательности [4].

4. *Метод наименее значимого бита (LSB).* Метод заключается в замене последнего значащего бита в исходном файле на биты сообщения, которое надо скрыть. В результате подмены полученный файл должен быть не отличим от оригинала человеческими органами восприятия.

   Преимущества:
   - простота реализации;
   - высокая емкость;
   - быстрая обработка, подходит для реального времени и маломощных устройств.

   Недостатки:
   - низкая устойчивость к атакам;
   - чувствительность к преобразованиям;
   - при неправильном выборе носителя или чрезмерной нагрузке данные становятся заметными [5].

III. Методы преобразования области определения

1. *Дискретное косинус-преобразование (ДКП).* Данный метод преобразует блоки изображения из пространственной области в частотную, что делает их более надежными по сравнению с методами во временной области, включая сжатие, обрезку и некоторые алгоритмы обработки изображений.

   Преимущества:
   - устойчивость к сжатию, метод совместим с JPEG;
   - гибкость внедрения.

   Недостатки:
   - сложность реализации;
   - ограниченная емкость, в каждый блок можно внедрить лишь небольшое количество информации;
   - уязвимость к фильтрации.

2. *Дискретное вейвлет-преобразование (ДВП).* Инкапсуляция сообщения с помощью ДВП дает хорошие результаты, которые превосходят методы ДКП. Вейвлет-преобразование разлагает изображение на поддиапазоны частот: низкие частоты по горизонтали и вертикали (основная структура изображения) и высокочастотные компоненты, содержащие детали и шум.

   Преимущества:
   - высокая скрытность ;
   - устойчивость к сжатию и фильтрации;
   - совместимость с кодами коррекции ошибок;

   Недостатки:
   - сложность реализации;
   - ограниченная емкость, внедрение больших объёмов данных может повлиять на качество изображения;
   - чувствительность к обработке [3].

IV. Заключение

В данной статье были рассмотрены некоторые из основных методов стеганографии изображений для временной области и преобразования области определения. Исходя из проведенного анализа следует отметить, что различные форматы графических файлов имеют свои методы для сокрытия информации, которые в свою очередь имеют сильные и слабые стороны.

Выбор метода стеганографии зависит от конкретных требований и условий применения. Таким образом, если важна простота и скорость, можно использовать LSB метод, для усложнения извлечения без изменения структуры – псевдослучайные перестановки, для изображений с высокой степенью защиты и устойчивостью к атакам – метод ДКП или ДВП. Преобразование ДКП или ДВП более надежно, потому что позволяет скрыть сообщение в области частот. Данная область менее подвержена зрению человека. С точки зрения развития методов стеганографии, интересен подход, основанный на перестановке битов, замене старших и младших разрядов.

V. Список литературы

1. Грибунин, В. Г. Стеганография, цифровые водные знаки и стегоанализ / В. Г. Грибунин // – М.: Вузовская книга, 2018. – 110 с.
2. Грибунин, В. Г. Цифровая стеганография. Аспекты защиты / В. Г. Грибунин, И. Н. Оков, И. В. Туринцев // – М.: Солон-Пресс, 2009. – 264 с.
3. Пономарев, И. В. Стеганографические методы встраивания и обнаружения сокрытых сообщений, использованых GIF-изображения в качестве файлов-контейнеров/ И. В. Пономарев, Д. И. Строкин // Известия Алтайского государственного университета. –2022. –№1(123).– с. 112-115.
4. Земцов, А. Методы цифровой стеганографии для защиты авторских прав / А. Земцов, // – М.: LAP Lambert Academic Publishing, 2019. – 148 с.
5. Рассел, Дж. Стеганография / Дж. Рассел, // – М.: VSD, 2019. – 193 с.