Примером выходной информации является каталог доступных помещений.

Программное средство включает в себя работу с базой данных, серверную и клиентскую часть. В качестве базы данных используется MySQL. Серверная часть написана на объектно-ориентированном языке PHP с использованием Yii фреймворка 2-й версии. Для обработки нагруженных операций (обработка загружаемых изображений, рассылка уведомлений о новой заявке на бронирование) используется сервер очередей beanstalkd. Клиентская часть представляет собой реализацию hamaterialize.css фреймворк использованием JQuery библиотеки.

УДК 004.056.03

Студ. А.А. Боровик
Науч. рук. доц. Н. В. Пацей
(кафедра информационных систем и технологий, БГТУ)

ПРАКТИЧЕСКИЕ МЕТОДЫ СКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ ГРАФИЧЕСКОЙ СТЕГАНОГРАФИИ

В настоящее время, проблема обеспечения конфиденциальности хранимых и, особенно, пересылаемых данных стала чрезвычайно острой. Наиболее очевидным решением проблемы защиты и сокрытия информации является шифрование. То есть представление данных в таком виде, в котором, не зная ключа, их невозможно было бы понять. Эти данные можно более или менее безопасно хранить и пересылать по общедоступным каналам связи. Такой способ защиты информации, называемый криптографической защитой (криптографией), широко используется как в компьютерной, так и в других сферах жизни человеческого общества. Цель криптографии состоит в блокировании несанкционированного доступа к информации путем шифрования содержания секретных сообщений. Однако существуют и иной метод обеспечения конфиденциальности данных – стеганографическая защите (стеганография).

Идея стеганографии состоит в том, чтобы скрыть сам факт сокрытия какой-либо информации. В отличие от криптографии, которая скрывает содержимое секретного сообщения, стеганография скрывает сам факт его существования. Как правило, сообщение будет выглядеть как что-либо иное, например, как изображение, статья, список покупок, письмо или судоку. Стеганографию обычно используют совместно с методами криптографии, таким образом, дополняя её. Преимущество стеганографии над чистой криптографией

состоит в том, что сообщения не привлекают к себе внимания. Сообщения, факт шифрования которых не скрыт, вызывают подозрение и могут быть сами по себе уличающими в тех странах, в которых запрещена криптография. Таким образом, криптография защищает содержание сообщения, а стеганография защищает сам факт наличия каких-либо скрытых посланий.

В настоящее время методы компьютерной стеганографии развиваются по двум основным направлениям: методы, основанные на использовании специальных свойств компьютерных форматов; методы, основанные на использовании избыточности аудио и визуальной информации.

Среди методов графической стеганографии на практике широко применяются следующие: использование метаданных, а также замена наименее значащего бита.

Очень многие форматы могут хранить определенные метаданные. Плюс этого способа в том, что он так же не нарушает формат файла, а также работа с этими мета-данными обычно хорошо задокументирована. Почти все медиа-форматы имеют поддержку метаданных. Однако далеко не всегда там можно хранить данные так, чтоб их не было видно. У форматов JPEG, AVI и др. есть поддержка EXIF тэга. Данные в этом тэге хранятся парами ключ=значение. В теории нет никаких проблем добавить туда какой то не стандартный ключ содержащий ваши зашифрованные данные. Программа работающая с этим тэгом, наткнувшись на этот ключ, скорей всего просто проигнорирует его.

Суть метода замены наименее значащего бита (Least Significant Bits - LSB) заключается в сокрытии информации путем изменения последних битов изображения, кодирующих цвет на биты скрываемого сообщения. Разница между пустым и заполненным контейнерами должна быть не ощутима для органов восприятия человека.

Таблица 1 - Сравнительные характеристики стеганографических методов

Стеганографические методы	Описание	Недостатки	Преимущества
1. Методы использования специальных свойств компьютерных форматов данных			
1.1.Методы использования зарезервированных для расширения полей компьютерных форматов данных	Поля расширения имеются во многих мультимедийных форматах, они заполняются нулевой информацией и не учитываются программой	Низкая степень скрытности, передача небольших ограниченных объемов информации	Простота использования
1.2.Методы специального форматирования текстовых файлов:			
1.2.1.Методы использования известного смещения слов, предложений, абзацев	Методы основаны на изменении положения строк и расстановки слов в предложении, что обеспечивается вставкой дополнительных пробелов между словами	1.Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
1.2.2. Методы выбора определенных позиций букв (нулевой шифр)	Акростих – частный случай этого метода		
1.2.3.Методы использования специальных свойств полей форматов, не отображаемых на экране	Методы основаны на использовании специальных "невидимых", скрытых полей для организации сносок и ссылок		
1.3. Методы скрытия в неиспользуемых местах гибких дисков	Информация записывается в обычно неиспользуемых местах ГМД (например, в нулевой дорожке)	1.Слабая производительность метода, передача небольших объемов информации 2. Низкая степень скрытности	Простота использования. Имеется опубликованное программное обеспечение реализации данного метода
2. Методы использования избыточности аудио и визуальной информации			
2.1. Методы использования избыточности файлов цифрового видеоряда, фотографий или цифрового звука	Младшие разряды цифровых отсчетов содержат очень мало полезной информации. Их заполнение дополнительной информацией практически не влияет на качество восприятия.	С изменением информации искажаются статистические характеристики цифровых потоков,требуется коррекция статистических характеристик.	Возможность скрытой передачи большого объема информации. Возможность защиты авторского права, скрытого изображения, товарной марки и т.п.

Рисунок 5- метод LSB

Перечисленные выше методы достаточно просты в реализации, а также находят широкое применение. Однако они обладают существенным недостатком – они легко поддаются стегоанализу. Это обусловлено тем, что для передачи сообщения возникает необходимость модификации стегоконтейнера, что может быть обнаружено при помощи современных методов стегоанализа.

В качестве решения данной проблемы предлагается метод хеш-стеганографии. Данный метод абсолютно не подвержен стеганографическому анализу. Это обусловлено тем, что для передачи или хранения используются пустые (неизменённые) стегоконтейнеры. Скрываемая информация содержится в хеш-кодах (определённые части значений хеш-функции от файла-контейнера). Стегоключом в данном методе является длина хеш-кода, а также его смещение относительно начала значения хеш-функции.

Однако данный метод имеет также и значительные недостатки – объём данных, которые могут быть скрыты в стегоконтейнере, ограничивается размером значения хеш-функции, что даёт значительно меньшие возможности по сокрытию информации по сравнению с другими методами. Кроме того, подбор необходимого контейнера требует наличия большой базы данных, а также может занимать значительное время. Данный метод идеально подходит для случаев, когда объём передаваемой информации невелик, но в то же время требуется высокая секретность.

ЛИТЕРАТУРА

1. Конахович Г. Ф., Пузыренко А. Ю. Компьютерная стеганография. Теория и практика. — К.: МК-Пресс, 2006. — 288 с.

2. Грибунин В. Г., Оков И. Н., Туринцев И. В. Цифровая стеганография. — М.: Солон-Пресс, 2002. — 272 с.

3. Рябко Б. Я., Фионов А. Н. Основы современной криптографии и стеганографии. — 2-е изд. — М.: Горячая линия — Телеком, 2013. — 232 с.

4. Завьялов С.В., Ветров Ю.В. Стеганографические методы защиты информации.