Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г.ЧЕРНЫШЕВСКОГО»

Кафедра дискретной математики
и информационных технологий

Применение стеганографии для обнаружения скрытой информации в графических файлах

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студентки 4 курса 421 группы
направления 09.03.01 «Информатика и вычислительная техника»
факультета компьютерных наук и информационных технологий
Кульбаевой Ирины Руслановны

Научный руководитель
к. ф.-м.н., доцент _____ И.Д. Сагаева

Заведующий кафедрой
к. ф.-м.н., доцент _____ Л.Б. Тяпаев

Саратов 2016

Введение. Широкое использование стеганографии, а также ее открытый доступ в Интернете, повлекли за собой проблему передачи незаконного материала, скрытого в графических, ауди и других форматах. Стеганография также может быть использована как способ организации утечки ценной информации из компаний и т.д. Поэтому развитие методов стеганоанализа на сегодняшний день является чрезвычайно актуальной задачей.

Целью выпускной работы является создание сайта, реализующего встраивание/извлечение скрытого сообщения в bmp-изображении, а также шифрование сообщения. Для достижения цели были выделены и решены следующие подзадачи:

- Изучен теоретический материал по стеганоанализу, основам HTML верстки, разработки сайта;
- HTML верстка;
- авторизация, с подключением SQLite;
- шифрование криптосистемой Виженера и RSA;
- реализация алгоритма встраивания сообщения (LSB);
- RS анализ изображения на наличие встроенного сообщения с последующем его дешифрованием.

Структура выпускной квалификационной работы состоит из введения, трех глав, заключения и списка использованных источников.

В первой главе дается общее представление о стеганографии и стеганоанализе.

Во второй главе подробно описаны конкретные методы обнаружения, такие как, визуальное обнаружение, обнаружение на основе анализа гистограммы, методы статистики с использованием пространственной корреляции и тд.

В третьей главе реализована практическая часть, то есть создание сайта стегошифратора/стегодешифратора.

1 Стеганография. Стеганография в переводе с греческого означает тайнопись (steganos - секрет, тайна; graphy - запись). Главная задача стеганографии — это сокрытие факта передачи информации и существование секретного послания.

Эффективность стеганографического метода определяется максимальным объемом встраиваемой информации, сложностью алгоритма встраивания и извлечения сообщений, а также устойчивостью к стегоанализу.

Схема встраивания состоит из двух основных этапов:

• первый – формирование рабочей области контейнера и формирование битового блока;

• второй – процесс встраивания передаваемого сообщения в контейнер (формирование стего-контейнера).

Задачей первого этапа является формирование рабочей области контейнера, куда будет производиться встраивание информации. Для современных методов характерен подход, при котором контейнер делится на две части (зоны), а при встраивании используется только одна из них. Основной задачей на втором этапе является разработка метода встраивания передаваемого сообщения в сформированную рабочую область контейнера путем внесения изменений в сформированный битовый блок. При этом решается задача обеспечения незаметности факта встраивания. Незаметность искажений принято оценивать отношением количества искаженных бит в битовом блоке к его объему. Чем большее значение имеет этот параметр, тем менее эффективным считается предлагаемый метод [3, 4].

В 1996 году на конференции Information Hiding: First Information Workshop была принята единая терминология:

- Стеганографическая система (стегосистема) — объединение методов и средств используемых для создания скрытого канала для передачи информации.

– Сообщение — это термин, используемый для общего названия передаваемой скрытой информации.
– Контейнер — так называется любая информация, используемая для сокрытия тайного сообщения.
– Стеганографический канал (стегоканал) — канал передачи стегоконтейнера.
– Ключ (стегоключ) - секретный ключ, нужный для сокрытия стегоконтейнера [3].

Все множество методов для стеганографии можно разделить на две категории, работающие в области изображения (Image Domain) или в области преобразований (Transform Domain).

1. Инструменты области изображения манипулируют младшим значащим битом (LSB) или шумом в изображении. Такой подход типичен для стеганографии, и считается «простой системой» [limits].

Обычно используются форматы без потерь, данные могут быть напрямую восстановлены.

2. Инструменты области преобразований манипулируют алгоритмами и преобразованиями изображения, такими как DCT (Дискретное косинусное преобразование), используемое в JPEG, или широкополосным (импульсным, wavelet) преобразованием.

Эти методы более тесно интегрированы с форматом обложки и алгоритмом сжатия, используемым, для уменьшения избыточности обложки (JPEG, MPEG-video, MP3-audio) – такие алгоритмы дают результат, находящийся ниже порога восприятия человека, но выше уровня, где начинается «избыточность», отбрасываемая алгоритмами сжатия (могут использоваться модели основанные на особенностях восприятия человека – например, в течение некоторого времени после громкого звука мы не можем услышать тихий звук, играющий фоном). Эти методы скрывают информацию в более значительных объёмах (или площадях) «обложки» и могут

затрагивать статистические свойства «изображения», такие как яркость, громкость и т.п. [7].

2 Методы стеганоанализа. Стеганоанализ – искусство и наука, параллельно развивающаяся со стеганографией.

Стеганоанализ осуществляет поиск и анализ определенных характеристик и признаков в исследуемом цифровом объекте, установление факта наличия или отсутствия которых позволяет получить ответ на вопрос, является ли анализируемый объект стеганосообщением или же он не подвергался преобразованию.

Основной целью стеганоанализа является моделирование стеганографических систем и их исследование для получения качественных и количественных оценок надежности использования стеганопреобразования, а также построение методов выявления скрываемой в контейнере информации, ее модификации или разрушения.

Проведенный анализ существующих методов стеганоанализа показал, что в зависимости от *используемых исходных данных* их можно разделить на две основные группы:

1. Методы, предназначенные для работы с конкретными заранее известными стеганографическими алгоритмами.
2. Методы, предназначенные для любых алгоритмов стеганографии.

Рассмотрим подробнее вторую группу.

Обнаружение наличия скрытой информации состоит из субъективных и статистических методов.

Субъективные методы использует человеческое зрение, чтобы обнаружить подозрительные различия на изображении.

Одним из субъективных методов являет алгоритм Ezstego. Данный алгоритм встраивания последовательно встраивает скрытое сообщение в палитре индексами GIF изображений.

Еще одним распространённым методом является визуальный анализ. Он базируется на способности зрительной системы человека анализировать зрительные образы и выявлять существенные различия в сопоставляемых изображениях. Основная идея метода заключается в сравнении изображения в целом с изображениями его битовых срезов, [5].

Статистические методы осуществляются с помощью математического анализа изображений, чтобы найти расхождение между оригиналом и стегоизображенем.

Первый статистический метод специфической детекции основан на статистическом анализе из выборочных значений в парах. Известно, хи - квадрат атаки, которые обеспечивает точное обнаружение сообщения, последовательно вставленного в картинку. Хотя этот метод является успешным в случае для последовательного вложения или большого сообщения.

Одним из оригинальных методов статистического стеганоанализа является метод RS анализ. Сокращение в названии расшифровывается как *Regular-Singular,* то есть «регулярно-сингулярный» [1].

RS Анализ может обеспечить надежное и точное обнаружение случайно внедренного сообщения. Изображение разбивается на "регулярные" или "сингулярные" группы в зависимости от шума данной группы. Доля «регулярных» и «сингулярных» групп образует кривые, квадратичные в размере встроенного сообщения. Если некоторые предположения удовлетворены, длина сообщения может быть точно оценена.

Еще один эффективный метод Анализа пар. В 2003 году Думитреску, У и Ван (Dumitrescu, Wu, Wang) предложили метод анализа сокрытий заменой наименее значащих битов отсчетов пространства сокрытия (под пространством сокрытия понимаем набор элементов используемого в качестве контейнера информационного объекта, путем модификации которых производится сокрытие с помощью рассматриваемого метода),

также пригодный в случае псевдослучайного "размазывания" битов сообщения по отсчетам контейнера [1].

Этот метод, известный как "Анализ пар значений" (Sample Pair Analysis, "SPA") является фактически обобщением RS-анализа и его формулировкой в несколько других терминах, более удобных для строгих доказательств, лежащих в основе метода принципов. Позже метод SPA многократно развивался и обобщался. Современные версии метода обладают достаточно высокой эффективность.

3 Практическая часть. Целью практической части выпускной работы является создание функционирующего сайта, реализующего встраивание/извлечение скрытого сообщения в bmp-изображении.

При встраивании сообщения используется алгоритм LSB (least significant bits), который состоит в перезаписи младших бит изображения, а также шифрование несколькими криптосистемами (Виженера, RSA BSAFE). Одной из особенностью сайта является возможность не только блочного встраивания сообщения, но и рандомного распределения бит.

Для извлечения сообщения используется RS анализ, направленный на выявление скрытых зависимостей между элементами контейнера. Также, на правах администратора, возможен вывод результатов анализа на экран.

При выполнении работы потребовалось:

- HTML верстка сайта;
- регистрация, авторизация с подключением SQLite сервера;
- шифрование криптосистемой Виженера и RSA BSAFE;
- реализация алгоритма встраивания сообщения (LSB);
- стеганоанализ изображения на наличие встроенного сообщения с последующем его дешифрованием.

Большая часть работы выполнена на языке программирования JavaScript. RS анализ реализован на языке Java.

В ходе детального изучения данных и многократного тестирования была выявлена некоторая закономерность. Для стегодетектора менее заметным является то сообщение, которое встраивалось при помощи равномерного распределения скрытого сообщения по контейнеру, а также на заметность влиял объём встраиваемой информации и файла-контейнера.

Заключение. В данной работе были рассмотрены наиболее популярные методы стеганографии, а также субъективные и статические методы стеганоанализа. За время работы над выпускным проектом был изучен теоретический материал по стеганоанализу, основам HTML верстки, разработки сайта.

Результатом работы является создание сайта, который реализует встраивание/извлечение скрытого сообщения в BMP изображение. Встраивание реализовывалось с помощью метода LSB. В качестве шифрования сообщения был выбран шифр Виженера и RSA BSAFE. Для создания были использованы следующие технологии:

- основная часть разработана на платформе Nodejs с использованием базы данных SQLite;
- HTTP сервер реализован с помощью Express.js фреймворка;
- работа с базой данных осуществляется с помощью Sequelize ORM;
- клиентская часть реализуется как одностраничное SPA (Single Page Application) приложение, написанное на HTML5/CSS3 для верстки и Javascript для программирования клиентской части;
- RS анализ реализован на языке Java. Сборка Java кода производилась в jar приложении.

Список использованных источников

1 Chen W. Study of steganalysis methods //Department of Electrical and Computer Engineering, New Jersey 2005

2 Беззатеев С.В., Волошина Н.В., Жиданов К.А.: Специальные классы кодов для стеганографических систем. УДК 681.322 – 2012.

3 Pfitzmann B. Information Hiding Terminology// Information Hidding, Springer Lecture Notes of Computer Sciense. – 1996. – С. 347-350

4 Зорин Е.Л., Чичварин Н.В., Стеганография В САПР//Учебно-методическое пособие. - Москва.

5 Алиев А.Т. О применении стеганографического метода LSB к графическим файлам с большими областями монотонной заливки / А.Т. Алиев // Вестник ДГТУ. – Ростов-на-Дону, 2004. – Т. 4, № 4 (22). – С. 454-460.

6 И.В. Швидченко. Методы стеганоанализа для графических файлов// Институт кибернетики имени В.М. Глушкова // НАН Украины, г. Киев

7 Васина Т. С. Обзор современных алгоритмов стеганографии.// Электронное научно- техническое издание «Наука и Образование» - # 04, апрель 2012

8 Westfeld A., Pfitzmann A. Attacks on Steganographic Systems Breaking the Steganographic Utilities EzStego, Jsteg, Steganos, and S-Tools—and Some Lessons Learned.// Dresden University of Technology Department of Computer Science D-01062 Dresden, Germany

9 В.Г. Грибунин, И. Н. Оков, И. В. Туринцев. Цифровая стеганография. – М., Солон-пресс. 2002.