Учреждение образования

«Белорусский государственный технологический университет»

**Отчет к лабораторной работе № 13**

по дисциплине «Защита информации и надежность информационных систем»

Выполнил:

Студент 3 курса 1 группы ФИТ

Парибок Илья Александрович

2023 г.

**Исследование методов текстовой стеганографии**

**Цель:** изучение стеганографических методов встраивания/извлечения тайной информации с использованием электронного файла-контейнера текстового формата, приобретение практических навыков программной реализации методов (рассчитана на 4 часа аудиторных занятий: 2 часа – часть 1, 2 часа – часть 2).

**Задачи:**

1. Закрепить теоретические знания из области текстовой стеганографии, классификации, моделирования стеганосистем подобного вида и сущности основных методов.

2. Изучить основные алгоритмы встраивания/извлечения тайной информации на основе методов текстовой стеганографии, получить опыт практической реализации методов.

3. Разработать приложение для реализации алгоритмов встраивания/извлечения тайной информации на основе методов текстовой

стеганографии.

4. Познакомиться с методиками оценки стеганографической стойкости методов.

5. Результаты выполнения лабораторной работы (отдельно по каждой из 2 частей) оформить в виде описания разработанного приложения (для части 2), методики выполнения экспериментов с использованием приложений и результатов экспериментов.

**Теоретические сведения**

Для понимания сущности некоторых из методов полезно познакомиться с важнейшими особенностями и параметрами использования стилей (в том числе пространственно-геометрическими параметрами шрифтов), на основе которых строится текстовый файлконтейнер. На рисунке 1 показаны основные из параметров шрифта.

Изображение выглядит как текст, Шрифт, снимок экрана, диаграмма

Автоматически созданное описание

Рисунок 1 – Параметры шрифта

К синтаксическим методам компьютерной стеганографии, которые характеризуются сравнительно невысокой эффективностью (с точки зрения объема встраиваемой информации), относятся следующие (такие методы мы отнесем к числу базовых синтаксических методов):

• изменение расстояния между строками электронного текста (Line-Shift Coding); называется методом изменения межстрочных интервалов; сущность заключается в том, что используется текст с различными межстрочными расстояниями: выделяется максимальное и минимальное расстояния между строками, позволяющее кодировать соответственно символы «1» и «0» осаждаемого сообщения;

• изменение расстояния между словами в одной строке электронного текста (Word-Shift Coding); суть метода состоит в том, что осаждение информации основано на модификации расстояния между словами текста-контейнера; • изменение количества пробелов между словами (частный случай метода Word-Shift Coding); основан на том, что, например, чередование одинарного пробела и двойного (хх\_хх\_\_хх) кодирует «1», переход же с двойного пробела на одинарный кодирует «0» (хх\_\_хх\_хх);

 • на основе внесения специфических изменений в шрифты, т. е.начертания отдельных букв (Feature Coding); заключается в изменении написания отдельных букв используемого стандартного шрифта: визуально заметны различные образы, соответствующие буквам с верхними (например, l, t, d) или нижними (например, a, g) выносными элементами (см. рис. 1); например, букву «А» можно модифицировать, незначительно укорачивая длинную нижнюю часть буквы (рис. 2);

Изображение выглядит как зарисовка, дизайн, черно-белый

Автоматически созданное описание

Рисунок 2 – Пример применения метода Feature Coding:

а – пустой контейнер; б – заполненный контейнер

• изменение интервала табуляции; аналогичен вышеописанному методу изменения количества пробелов, только в этом случае меняется не количество пробелов, а соответственно расстояние между строками и интервал табуляции;

• Null Chipper (дословно – несуществующий, нулевой лепет); предполагает размещение тайной информации на установленных позициях слов или в определенных словах текста-контейнера, который, как правило, лишен логического смысла (как видно, действительно лепет);

• увеличение длины строки; предусматривает искусственное увеличение длины каждой строки за счет пробелов: например, нет пробела (определяется положением знака перехода на новую строку) – «0», один пробел – «1»;

• использование регистра букв; для обозначения бита секретного сообщения, представленного единицей, используется символ нижнего регистра, а нулем – верхнего (или наоборот);

• использование невидимых символов; знак «пробел» кодируется символом с кодом 32, но в тексте его можно заменить также символом, имеющим код 255 (или 0), который является «невидимым» и отображается как пробел.

Рассмотренные базовые методы могут применяться независимо и совместно, сохраняют исходный смысл текста, а обеспечиваемые ими показатели плотности кодирования при совмещении складываются. Еще одна важная особенность. Перечисленные методы работают успешно до тех пор, пока тексты представлены в коде ASCII.

Существуют также стеганографические методы, которые интерпретируют текст как двоичное изображение. Необходимо отметить, что данные методы не чувствительны к изменению масштаба документа, что обеспечивает им хорошую устойчивость к большинству искажений, которые могут иметь место при активных атаках. К числу основных лингвистических методов относятся [2, 52]:

 • метод синонимов; в качестве примера приведем подмножество синонимов: {«тайный», «секретный», «конфиденциальный», «доверительный»}. В приведенном подмножестве каждое слово имеет единственное одинаковое смысловое значение, что позволяет закодировать каждое слово своим уникальным кодом (т. е. выполнить операцию осаждения), например, «доверительный» – 00, «конфиденциальный» – 01, «секретный» – 10, «тайный» – 11. Подобное кодирование позволяет выбирать одно из четырех слов (как видим, они для удобства расположены по алфавиту) в зависимости от двух битов секретного сообщения. Отметим, что при этом, независимо какое из четырех слов будет выбрано, семантика сообщения не изменится. Очевидно, что при этом количество символов, соответствующих одному из синонимов используемого подмножества, зависит от общего числа элементов в подмножестве. Кроме того, обеим сторонам стеганосистемы должен быть известен общий алгоритм кодирования, т. е. один из ключей системы. Следует отметить, что в каждом подмножестве синонимов их упорядочивание должно выполняться по одному и тому же алгоритму и у отправителя сообщения, и у его получателя. В случае наличия слов с несколькими смысловыми значениями подобное кодирование оказывается невозможным. Также невозможно кодирование, если один из синонимов состоит из двух (или более) разделенных пробелом слов;

• метод переменной длины слова; основан на том, что длина слов в сообщении зависит от содержания секретного сообщения и способа кодирования слов: обычно одно слово текста-контейнера определенной длины кодирует два бита информации из стеганосообщения; например, слова текста длиной в 4 и 8 символов могут означать комбинацию битов «00», длиной в 5 и 9 – «01», 6 и 10 – «10», 7 и 11 букв – «11»; слова короче 4 и длиннее 11 букв можно вставлять где угодно для лексической и грамматической связки слов в предложении – программное приложение, которое декодирует принятое сообщение (извлекает сообщение из стеганоконтейнера), будет просто игнорировать их;

• метод первой буквы – программа-помощник в этом методе накладывает ограничение уже не на длину слова, а на первую (можно на вторую) букву; обычно одну и ту же комбинацию могут кодировать несколько букв, например, комбинацию «101» означают слова, начинающиеся с «А», «Г» или «Т;

• мимикрия; мимикрия генерирует осмысленный текст, используя синтаксис, описанный в Context Free Grammar (CFG), и встраивает информацию, выбирая из CFG определенные фразы и слова; грамматика CFG – это один из способов описания языка, который состоит из статических слов и фраз языка, а также узлов.

**Метод на основе апроша**

Апрош определяет расстояние между соседними символами текста. Фактически апрош состоит из двух таких расстояний – полуапрошей, являющихся как бы пространством, прилегающим к каждому из символов-соседей (см. рис. 13.1 и 13.4). Мы далее будем обращаться только к апрошу. Согласно существующим техническим правилам набора нормальный апрош должен быть равен половине кегля (размера) шрифта. Идея метода [69, 70] заключается в следующем. Встраивание сообщения в контейнер может быть основано на модификации базового (устанавливаемого текстовым процессором по умолчанию) значения апроша ао, его изменением от базового до некоторого максимального аmax (или минимального аmin), которое зрительно не должно отличаться от стандартного. Такое изменение производится с определенным шагом (дискретно) Δаi, каждому значению которого присваивается определенный бит или определенная комбинация битов.

Изображение выглядит как текст, Шрифт, Графика, графический дизайн

Автоматически созданное описание

Рисунок 3 – Изменение Апроша

Изменение величины апроша между двумя определенными символами текста относительно базового значения ао на небольшое расстояние (пункты (пт) или доли пункта) формально можно представить в следующем виде: at = ао + Δаt. (13.1) Такое изменение не должно вызывать визуально заметного уплотнения (Δаt <0) или разрежения (Δаt>0) групп символов. В текстовом процессоре MS Word апрош может принимать значения в диапазоне от 0 до 1584 пунктов.

Особенностью рассматриваемого метода является возможность одноразового размещения (в апроше одного символа) числа битов, определяемого дискретной разницей между минимальным и максимальным значениями Δа. Например, если отсчет вести от Δаmin до установленного интервала Δаt в виде параметра 0,1 nд (пт), то количество условных дискретных единиц nд, представленное в бинарном виде, определяет число битов, которые можно таким образом разместить; например, Δаmin= –0,5 пт, а Δаt = 0,3 пт. Разница между этими величинами составляет 0,8 пт: 8 · 0,1 или nt = 8 (в двоичном виде – 1000; в первом приближении именно такую бинарную комбинацию можно разместить (осадить) путем модификации конкретного апроша). На этой основе могут быть разработаны различные варианты кодировки осаждаемых комбинаций.

**Метод на основе кернинга**

В текстовых документах встречаются такие сочетания знаков, которые образовывают визуальные «дыры» либо «сгущения». Например, в текстах на основе кириллицы – это такие сочетания: «ГА», «TA», «ATA», «ЬТ» и т. п., на основе латиницы – «AY», «AV», «T;», «ff», а на основе греческого алфавита – «ΘΑ», «ΔΟ», «λκ» и др. Такие сочетания называются кернинговыми парами. Особенности «кернингования» приведены на рис. 4. Под кернингом обычно понимается процесс изменения межсимвольного расстояние между отдельными парами символов или кернинговыми парами (именно фактор парности отличает кернинг от апроша).

**Изображение выглядит как текст, Шрифт, белый, Графика

Автоматически созданное описание**

Рисунок 4 – Пояснение к понятию кернинга

Таким образом, технология кернинга, появившаяся в полиграфии после внедрения фотонабора (а затем и компьютерного набора), включает подбор межбуквенных интервалов для конкретных пар букв с целью улучшения внешнего вида и удобочитаемости текста. Такой избирательный подбор позволяет компенсировать неравномерности визуальной плотности текста, получаемой при использовании стандартных апрошей для каждой буквы.

С появлением цифрового фотонабора стало возможным хранить такие критические сочетания знаков (кернинговые пары) для некоторого условного шрифта, общее число которых мы обозначим Nk, в памяти компьютера с указанием величины (σ), на которую необходимо сдвинуть символы, чтобы визуально выровнять буквенные просветы. Как правило, текстовые редакторы или процессоры содержат встроенные средства настройки кернинга, который определяет стандартный межбуквенный интервал для того или иного шрифта. При этом σ устанавливается в соответствии со значениями из таблицы кернинговых пар, встроенной в вышеуказанный файл со шрифтом. Такая настройка позволяет выровнять шрифт и является стандартной. В некоторых шрифтах сейчас количество пар доходит до нескольких тысяч. Значение кернинга может быть как положительным (когда знаки раздвигаются, σ > 0), так и отрицательным (когда сдвигаются, σ < 0). Эта величина в программах верстки устанавливается в процентах от ширины символа пробела используемого шрифта.

**Практическое задание**

Разработать авторское приложение, реализующее один из методов текстовой стеганографии на основе модификации пространственно-геометрических параметров текста-контейнера.

В соответствии с 11 вариантом в качестве реализуемого метода возьмем: модификация расстояния между строками. Сущность заключается в том, что используется текст с различными межстрочными расстояниями: выделяется максимальное и минимальное расстояния между строками, позволяющее кодировать соответственно символы «1» и «0» осаждаемого сообщения;

Каждый абзац документа получает свой межстрочный интервал, который кодирует двух битовую последовательность сообщения. Интервалы для каждого абзаца привязаны к битовым группам: 00 соответствует интервалу 1.0, 01 - 1.1, 10 - 1.2, 11 - 1.3. Перед кодированием сообщение переводится в бинарный вид и разбивается на группы по 2 бита. Абзацы с межстрочным интервалом 1.08 не учитываются при извлечении сообщения из контейнера. В конце контейнер с закодированным сообщением сохраняется по новому пути. Реализация алгоритма кодирования представлена на рисунке 1, функция принимает сообщение, контейнер и исходный файл с сообщением.

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 1 – Алгоритм кодирования

При открытии файла с сообщением моно проверить результат работы алгоритма, просмотрев междустрочный интервал для первого и второго абзаца (рисунок 2-3).

Изображение выглядит как текст, снимок экрана, программное обеспечение

Автоматически созданное описание

Рисунок 2 – Межстрочный интервал второго абзаца

Изображение выглядит как текст, программное обеспечение, снимок экрана, Шрифт

Автоматически созданное описание

Рисунок 3 – Межстрочный интервал первого абзаца

При сравнении двух файлов (рисунок 4), человеческому взгляду сложно заметить разницу, а значит реализация имеет право на существование.

Изображение выглядит как текст, снимок экрана, Шрифт, алгебра

Автоматически созданное описание

Рисунок 4 - Сравнение контейнера до и после осаждения

При извлечении закодированного сообщения происходит анализ межстрочных интервалов каждого абзаца. Если интервал соответствует одному из значений, которые кодируют битовую группу, то соответствующие биты добавляются в буфер декодированного сообщения.

Изображение выглядит как текст, Шрифт, снимок экрана, линия

Автоматически созданное описание

Рисунок 5 – Результат вытягивания

**Вывод:**

В результате выполнения лабораторной работы были освоены методы текстовой стеганографии и созданы приложения, которые используют расстояния между строками для скрытия информации в тексте.

**Контрольные вопросы**

**1. В чем состоит сущность методов текстовой стеганографии?**

Сущность методов текстовой стеганографии заключается в скрытом передаче информации внутри текстового сообщения таким образом, чтобы наблюдатели не могли заметить наличие скрытой информации. Текстовая стеганография является одним из видов стеганографии, которая занимается сокрытием данных в текстовых документах.

Основные методы текстовой стеганографии включают в себя:

Метод замены символов: В этом методе используется замена определенных символов или слов в тексте скрытыми сообщениями. Например, можно использовать замену определенных букв или слов на их бинарные или шифрованные представления.

Метод пробельных символов: В этом методе информация скрывается в виде изменений в пробелах, переносах строки или других непечатаемых символах. Можно использовать различные алгоритмы для кодирования данных в этих пробельных символах.

Метод форматирования текста: здесь информация скрывается в изменении форматирования текста, таких как размер шрифта, стиль шрифта, цвет или выравнивание. Небольшие изменения в этих параметрах могут быть использованы для передачи скрытых данных.

Методы стеганографии с использованием словарей: В этом методе используется словарь или набор ключевых слов, которые служат для скрытой передачи информации. Например, можно использовать определенные слова или фразы в тексте, которые имеют специальное значение и сигнализируют о наличии скрытой информации.

Методы использования невидимых символов: В этом методе используются невидимые символы или символы с очень маленьким размером, которые не видны при обычном просмотре текста. Скрытая информация может быть закодирована в этих символах и извлечена с помощью специальных инструментов.

**2. Охарактеризовать методы синтаксической текстовой стеганографии. Привести примеры конкретной реализации методов.**

Синтаксическая текстовая стеганография основана на изменении синтаксической структуры текста для скрытой передачи информации. Вместо изменения символов или внешнего вида текста, как в других методах стеганографии, синтаксическая стеганография модифицирует грамматические правила или структуры предложений для внедрения скрытой информации. Это делает ее более устойчивой к атакам, поскольку изменения могут быть менее заметными.

Вот несколько методов синтаксической текстовой стеганографии:

Метод перестановки слов: В этом методе слова в предложении переставляются таким образом, что порядок слов сообщает скрытую информацию. Например, можно использовать кодирование сообщения в определенном порядке появления слов в предложении, в котором каждое слово имеет свою позицию, указывающую на скрытую информацию.

Пример: "Я сегодня купил яблоко" может стать "Купил сегодня яблоко я".

Метод изменения грамматической структуры: В этом методе грамматические конструкции и структуры предложений изменяются для скрытой передачи информации. Например, можно использовать изменение порядка слов или замену определенных частей речи для кодирования скрытого сообщения.

Пример: "Кот съел рыбу" может стать "Рыбу съел кот".

Метод вставки фиктивных предложений: В этом методе добавляются фиктивные предложения, которые выглядят как часть оригинального текста, но на самом деле содержат скрытую информацию. Например, можно использовать определенные ключевые слова или фразы, чтобы указать на наличие скрытой информации.

Пример: Оригинальный текст: "Он читал книгу. Она готовила обед." Модифицированный текст: "Он читал книгу. Приготовил свой обед сам."

**3. Охарактеризовать методы лингвистической текстовой стеганографии. Привести примеры конкретной реализации методов.**

Лингвистическая текстовая стеганография основана на использовании лингвистических особенностей языка для скрытой передачи информации. Этот подход использует различные лингвистические аспекты, такие как семантика, синтаксис, морфология или стилевые особенности, для внедрения и извлечения скрытой информации. Ниже приведены некоторые методы лингвистической текстовой стеганографии:

Метод использования семантических отношений: В этом методе скрытая информация кодируется с использованием семантических отношений между словами. Например, можно использовать синонимы или антонимы для замены слов в тексте, чтобы передать скрытую информацию.

Пример: Оригинальное предложение: "У него было плохое настроение." Модифицированное предложение: "У него было отвратительное настроение."

Метод стеганографии с использованием скрытых сообщений в морфологии слов: В этом методе скрытая информация кодируется путем изменения морфологических форм слов. Например, можно использовать изменение падежа, числа или времени слов для кодирования скрытого сообщения.

Пример: Оригинальное предложение: "Я купил красную розу." Модифицированное предложение: "Я купил красных роз."

Метод изменения стилевых особенностей: В этом методе стилевые особенности текста изменяются для скрытой передачи информации. Например, можно использовать изменение регистра слов (верхний/нижний), использование специфической лексики или стилизованных выражений для передачи скрытого сообщения.

Пример: Оригинальное предложение: "Это было интересное приключение." Модифицированное предложение: "Это было ШИКАРНОЕ приключение!"

**4. Дать оценку стеганографической стойкости методов текстовой стеганографии при конвертации текста-контейнера в иной текстовый формат.**

Оценка стеганографической стойкости методов текстовой стеганографии при конвертации текста-контейнера в другой текстовый формат зависит от нескольких факторов:

Видимость изменений: Методы, которые вносят минимальные изменения в исходный текст, обычно обладают более высокой стойкостью, поскольку изменения могут быть менее заметными для наблюдателя. Методы, которые изменяют грамматическую структуру или словоупотребление, могут быть менее стойкими, поскольку такие изменения могут привлечь внимание и вызвать подозрения.

Анализ стегосистемы: стойкость методов также зависит от возможности анализа стегосистемы, т.е. способности наблюдателя определить наличие скрытой информации. Некоторые методы могут быть уязвимы для статистического анализа или применения специальных алгоритмов для обнаружения скрытых сообщений. Более сложные методы, которые используют сложные стеганографические алгоритмы, обычно обладают более высокой стойкостью.

Изменение формата: Конвертация текста-контейнера в другой текстовый формат может повлиять на стойкость методов текстовой стеганографии. Некоторые форматы могут быть более устойчивы к изменениям или могут лучше сохранять структуру и особенности текста, что может снизить возможность обнаружения скрытой информации.

Оценка стойкости методов текстовой стеганографии при конвертации текста-контейнера в другой текстовый формат требует анализа каждого конкретного метода и его применения в конкретной ситуации. Некоторые методы могут быть более эффективными при определенных условиях, а другие - менее стойкими.

**5. Дать оценку стеганографической стойкости методов текстовой стеганографии при визуальном стеганоанализе текста-контейнера.**

Одним из популярных методов текстовой стеганографии является метод замены символов, когда символы в тексте-контейнере заменяются символами сообщения. Этот метод может быть достаточно простым и легко обнаруживаемым при визуальном стеганоанализе. Аналитик может заметить нереалистичные или неестественные текстовые паттерны, которые могут указывать на наличие скрытого сообщения.

Однако существуют и более сложные методы текстовой стеганографии, которые могут быть более стойкими и трудно обнаружимыми. Некоторые из таких методов включают изменение регистра символов, внедрение в пробелы или изменение интервалов между словами, использование незначащих символов и т. д. Эти методы могут усложнить задачу визуального стеганоанализа.

При оценке стеганографической стойкости методов текстовой стеганографии при визуальном стеганоанализе следует учитывать следующие аспекты:

Размер сообщения: чем больше сообщение, которое нужно скрыть, тем сложнее его обнаружить при визуальном анализе. Маленькие сообщения могут быть более стойкими, так как изменения в тексте-контейнере могут быть менее заметными.

Выбор метода стеганографии: Некоторые методы могут быть более устойчивыми к визуальному стеганоанализу, чем другие. Методы, которые изменяют только незначащие символы или используют сложные алгоритмы для замены символов, могут быть менее заметными и труднее обнаружимыми.

Используемые инструменты и алгоритмы стеганоанализа: Опытные аналитики, используя специализированные инструменты и алгоритмы, могут быть более успешными в обнаружении скрытых сообщений. Эффективность стеганоанализа зависит от доступных методов и технологий.

Уровень подозрительности: Визуальный стеганоанализ требует определенного уровня подозрительности и внимательности со стороны аналитика. Даже хорошо скрытое сообщение может быть обнаружено, если провести детальный анализ текста-контейнера.

**6. Дать общую характеристику стеганоанализу в области текстовой стеганографии на основе метода «χ-квадрат».**

Метод "χ-квадрат" (chi-square) является одним из распространенных методов стеганоанализа в области текстовой стеганографии. Он используется для обнаружения стеганографических изменений в текстовом контейнере путем анализа статистических отличий между ожидаемыми и фактическими частотами символов или других единиц информации.

Характеристики метода "χ-квадрат" в стеганоанализе текстовой стеганографии включают:

Статистический анализ: Метод "χ-квадрат" основан на математическом анализе статистических отличий. Он сравнивает ожидаемые и наблюдаемые частоты символов или других единиц информации в текстовом контейнере, чтобы определить наличие стеганографических изменений.

Чувствительность к статистическим отклонениям: Метод "χ-квадрат" чувствителен к статистическим отклонениям, которые могут возникнуть при внедрении скрытой информации. Если скрытое сообщение изменяет распределение символов или частоты, то это может быть обнаружено с помощью метода "χ-квадрат".

Уровень значимости: В методе "χ-квадрат" используется понятие уровня значимости для определения, насколько статистически значимы отличия между ожидаемыми и фактическими частотами. Высокий уровень значимости может указывать на наличие стеганографических изменений.

Применение к различным типам стеганографии: Метод "χ-квадрат" может применяться к различным типам текстовой стеганографии, где происходит изменение частот символов или других статистических свойств текста-контейнера.

Ограничения: Метод "χ-квадрат" не является универсальным и может иметь свои ограничения. Например, он может быть менее эффективным при стеганографии, которая применяет сложные алгоритмы для изменения частот или использует другие методы манипуляции текстом.

**7. Что такое апрош? В чем состоит сущность стеганометода на основе модификации апроша?**

Апрош (APROACH) — это метод стеганографии, который основан на модификации верхних бит (MSBs) цифрового изображения. Суть метода заключается в том, что информация скрывается путем изменения наименее значимых бит (LSBs) пикселей изображения в соответствии с битами сообщения.

Стеганометод на основе модификации апроша использует апрош как основную технику для внедрения скрытой информации в цифровое изображение. Он работает следующим образом:

Разделение изображения: Изображение разделяется на блоки пикселей, обычно размером 4x4 или 8x8.

Выбор целевых пикселей: В каждом блоке выбираются определенные пиксели для модификации. Эти пиксели обычно выбираются на основе их влияния на визуальное качество изображения.

Модификация LSBs: наименее значимые биты выбранных пикселей изменяются в соответствии с битами скрытого сообщения. Например, если бит скрытого сообщения равен 0, то LSB пикселя не изменяется; если бит равен 1, то LSB изменяется на противоположное значение.

Проверка воздействия: после модификации LSBs производится проверка воздействия на визуальное качество изображения. Если визуальные артефакты незаметны, то процесс продолжается; в противном случае, апрош может быть дополнительно модифицирован для снижения визуальных изменений.

Восстановление информации: при извлечении скрытого сообщения изображение анализируется для определения измененных LSBs пикселей, и на основе этих изменений восстанавливается скрытая информация.

**8. Что такое кернинг? В чем состоит сущность стеганометода на основе модификации кернинга?**

Кернинг (kerning) — это техника в типографии, которая относится к настройке промежутков между символами в тексте для достижения более равномерного и приятного визуального восприятия. Кернинг используется для коррекции проблем, связанных с визуальным выравниванием символов, такими как перекрытие или слишком большие промежутки между символами.

Сущность стеганометода на основе модификации кернинга заключается в использовании кернинга для внедрения скрытой информации в текстовый документ или шрифтовую информацию. Метод работает следующим образом:

Выбор символов и настройка кернинга: Определенные символы или их комбинации выбираются для модификации. Кернинг этих символов настраивается с целью создания "секретного шаблона" или кодового сообщения.

Модификация кернинга: Промежутки между символами в выбранных символах или комбинациях символов изменяются в соответствии с битами скрытого сообщения. Например, бит 0 может означать, что промежуток увеличивается, а бит 1 - что промежуток уменьшается.

Проверка визуальных артефактов: После модификации кернинга производится проверка визуальных артефактов. Если изменения в кернинге незаметны, то процесс продолжается; в противном случае, дополнительные шаги могут быть предприняты для снижения визуальных изменений.

Извлечение скрытой информации: При извлечении скрытой информации из текста или шрифтовой информации, кернинг анализируется для определения изменений промежутков между символами, и на основе этих изменений скрытая информация восстанавливается.

**9. Дать сравнительную оценку методов на основе модификации пространственно-геометрических и цветовых параметров символов текста-контейнера (критерий: отношение оправданного объема осаждаемой информации к объему контейнера).**

Сравнительная оценка методов на основе модификации пространственно-геометрических и цветовых параметров символов текста-контейнера в зависимости от отношения оправданного объема осаждаемой информации к объему контейнера может быть следующей:

Методы, основанные на модификации пространственно-геометрических параметров:

Оценка: Средняя

Объем осаждаемой информации: сравнительно низкий

Объем контейнера: Средний

Описание: Методы, основанные на изменении пространственно-геометрических параметров символов текста-контейнера, могут включать изменение размеров, формы, выравнивания символов и т. д. Они обычно обладают средним объемом осаждаемой информации и средним объемом контейнера. Однако, эти методы могут быть более устойчивыми к визуальному стегоанализу, так как изменения параметров символов могут быть менее заметными для человеческого восприятия.

Методы, основанные на модификации цветовых параметров:

Оценка: Высокая

Объем осаждаемой информации: сравнительно высокий

Объем контейнера: Средний до высокого

Описание: Методы, основанные на изменении цветовых параметров символов текста-контейнера, могут включать изменение яркости, насыщенности, оттенка и т. д. Они обычно обладают сравнительно высоким объемом осаждаемой информации и средним до высокого объема контейнера. Однако, эти методы могут быть более уязвимыми для визуального стегоанализа, так как изменения цветовых параметров могут быть заметными или влиять на общее визуальное восприятие текста.

**10. Какие новые методы текстовой стеганографии вы можете предложить?**

Вот несколько новых методов текстовой стеганографии, которые можно рассмотреть:

Методы, основанные на генерации синонимов: вместо прямой замены символов или битов используется генерация синонимов для замены определенных слов или фраз в тексте. Это может быть осуществлено с использованием методов обработки естественного языка (Natural Language Processing), аугментации текста или других техник.

Методы, использующие контекстные модели: Использование нейронных сетей и контекстных моделей для стеганографии текста. Нейронные сети могут быть обучены для внедрения скрытой информации в текстовые данные или для извлечения скрытой информации из текста.

Методы, основанные на распределении вероятностей: Эти методы используют статистические модели и распределение вероятностей для определения мест в тексте, где можно безопасно внедрить скрытую информацию. Могут быть использованы различные статистические меры, такие как информационная энтропия, распределение частот слов и другие.

Методы, основанные на кодировании и сжатии: В этом случае стеганография осуществляется путем применения различных методов кодирования и сжатия текста. Скрытая информация может быть внедрена в коды ошибок, замененные символы, сжатые данные и т. д.

Методы, использующие текстовые структуры: Эти методы используют специфические текстовые структуры, такие как таблицы, списки или разделы, для внедрения и извлечения скрытой информации. Например, скрытая информация может быть внедрена в заголовки или номера страниц.

Методы, основанные на контекстуальных маркировках: В этом случае текстовые данные могут быть помечены или размечены с использованием специальных символов или меток, которые указывают на наличие скрытой информации. Маркировки могут быть невидимыми для обычного наблюдателя и видимыми только для получателя, знающего секретный ключ