МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

**ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №13 НА ТЕМУ:**

Исследование методов текстовой стеганографии

Выполнил студент 3 курса 1 группы

Кашперко Василиса Сергеевна

2023 г.

Цель: изучение стеганографического метода встраивания/извлечения тайной информации с использованием электронного файла-контейнера текстового формата, приобретение практических навыков программной реализации методов.

Теоретические сведения

*Классификация, сущность и основные особенности базовых методов текстовой стеганографии*

К текстовой стеганографии относятся методы, предусматривающие использование в качестве контейнера файла-документа текстового типа.

Текстовая стеганография подразделяется на:

*Синтетические методы (затрагивают семантику текстового сообщения)*

– изменение расстояния между строками электронного документа;

– изменение расстояния между словами;

– изменение количества пробелов между словами;

– на основе внесения специфических изменения в шрифты;

– изменение интервала табуляции;

– Null Chipper (дословно – несуществующий, нулевай лепет);

– увеличение длины строки;

– использование регистра букв;

– использование невидимых символов.

*Достоинства*

– Легко применяются к любому тексту (независимо от содержания, назначения, языка);

– Легко реализуются в программном коде (т.к. они полностью автоматические)

*Недостатки*

– Невысокая эффективность (объем встраиваемой информации);

– Перечисленные методы работают успешно до тех пор, пока тексты представлены в коде ASCII;

– Неустойчивы к форматированию текса;

– Неустойчивы к изменению масштаба документа.

*Лингвистические методы (основаны на эквивалентной трансформации текстовых файлов-контейнеров)*

– Метод синонимов;

– Метод переменной длины слова;

– Метод первой буквы;

– Мимикрия.

Ход работы

Во время выполнения лабораторной работы было создано приложение, которое применяет подход в текстовой стеганографии с использованием библиотеки Spire.Doc.

Такое программное обеспечение позволяет зашифровать данные и внедрить их в файл Word, а также извлечь скрытую информацию из этого документа.

Интерфейс приложения показан на рисунке 1.

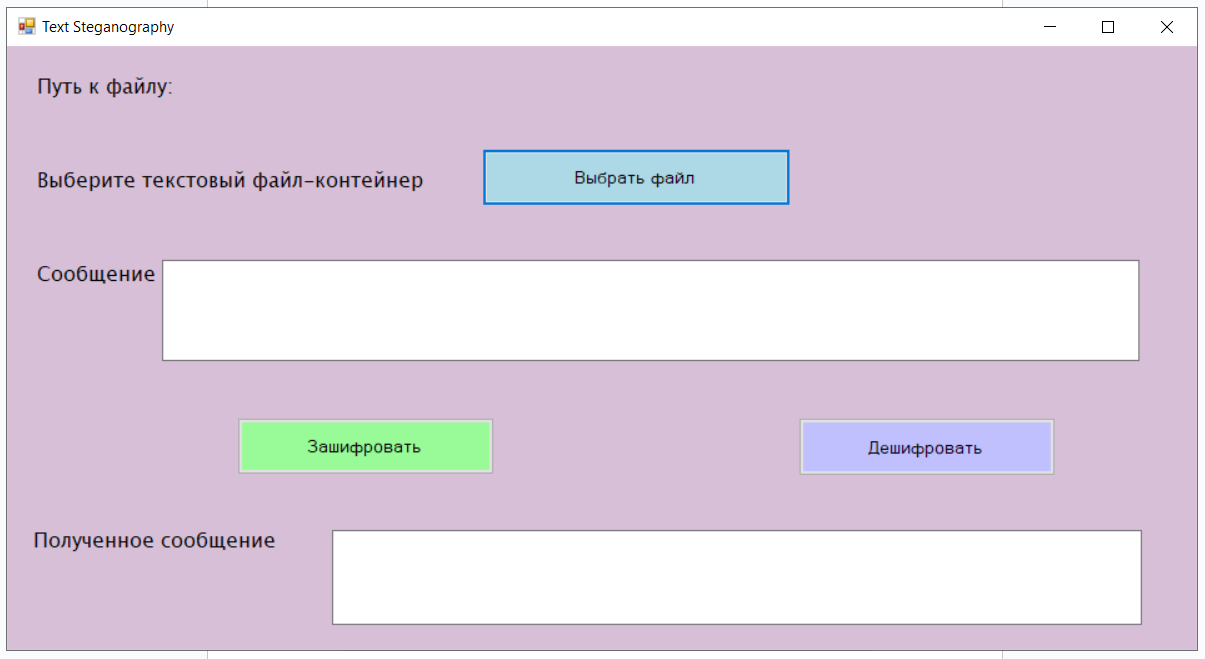


Рисунок 1 – Интерфейс приложения

*Зашифрование*

Для выполнения зашифрования информации для начала следует выбрать текстовый файл. При выборе файла открывается диалоговое окно с выбором файла. Для правильного выбора и предотвращения ошибок в программе диалоговое окно использует фильтры (рис. 2).

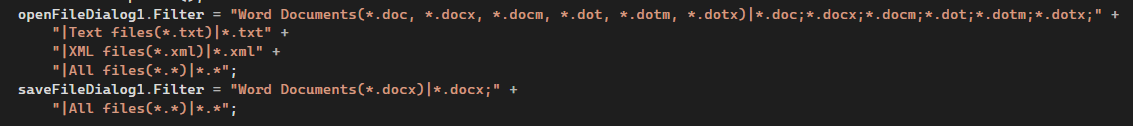


Рисунок 2 – Применение фильтров для выбора файла

После этого пользователю предлагается ввести сообщение, которое он хочет зашифровать в выбранном файле. Введенное сообщение преобразуется в последовательность байтов. Сначала сообщение конвертируется в коды ASCII, а затем каждый символ преобразуется в его бинарное представление.

Затем оригинальный текст документа загружается и разбивается на отдельные абзацы.

Для каждого абзаца случайным образом выбирается позиция, где будет произведена замена символа или слова. Замены осуществляются в соответствии с битовым представлением сообщения.

Если бит равен 1, символу устанавливается определенный отступ (-0.1f), а если бит равен 0, то применяется другой отступ (0.1f). Пробелы кодируются особым образом, с отступом 0.5f и выделением жирным шрифтом.

После вышеперечисленной операции осаждения информации в сообщение измененный документ сохраняется в новый файл формата .docx.

При визуальном просмотре документа изменения могут быть незаметны, но при проведении соответствующего анализа можно извлечь скрытое сообщение из документа с помощью специальной программы или скрипта.

*Расшифрование*

Пользователь выбирает зашифрованный документ, из которого требуется извлечь информацию.

Программа анализирует каждый абзац, исследуя отступы символов.

На основе этой информации происходит восстановление битовой последовательности, которая затем декодируется в исходное сообщение.

*Пример*

Для наглядного примера также к программной реализации добавлено изменение цвета символов, для которых изменяется отступ во время работы приложения.

Таким образом, символам устанавливается не только определенный отступ, но и цвет: для бита, равного 1 – цвет текста (AliceBlue), для бита, равного 0 – цвет (Pink).

Как и описывался алгоритм работы с приложением ранее, выполняем все действия пользователя.

Ниже изображена последовательность и результаты работы программы.

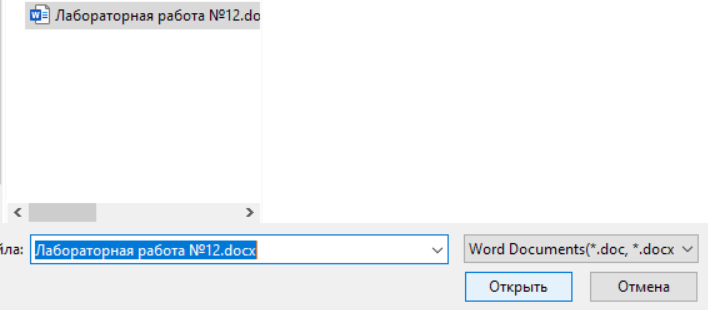


Рисунок 3 – Выбор файла-контейнера типа Word Documents

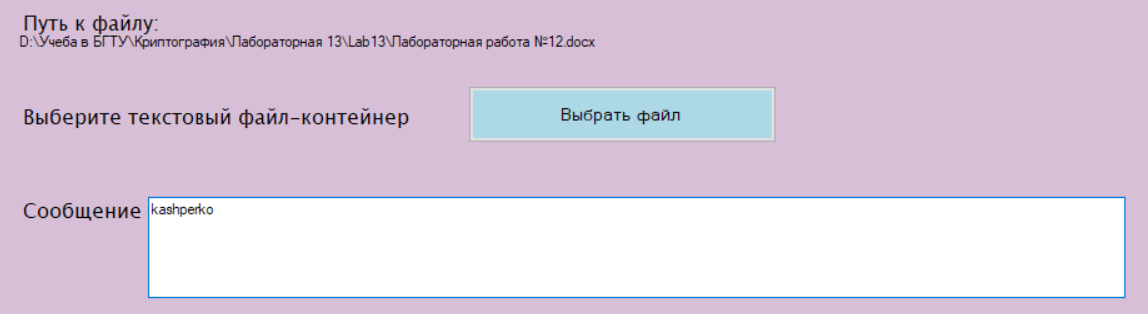


Рисунок 4 – Ввод сообщения для осаждения

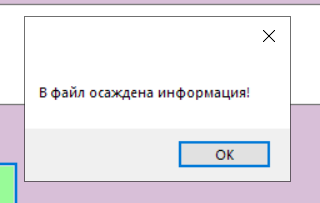


Рисунок 5 – Уведомление об успешном осаждении информации и сохранении измененного файла

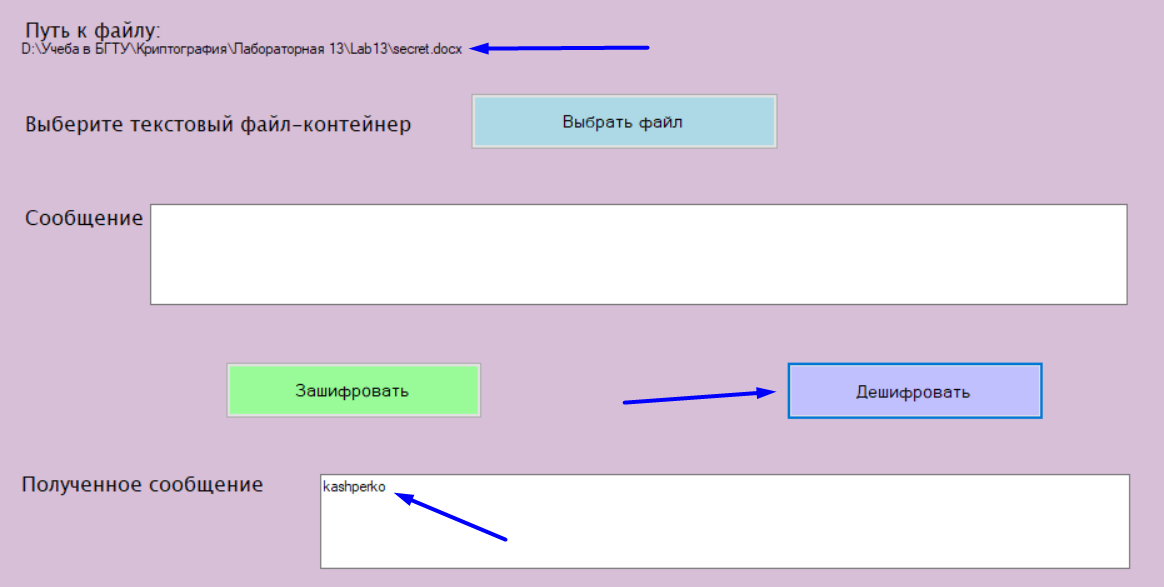


Рисунок 6 – Последовательность получения расшифрованного сообщения

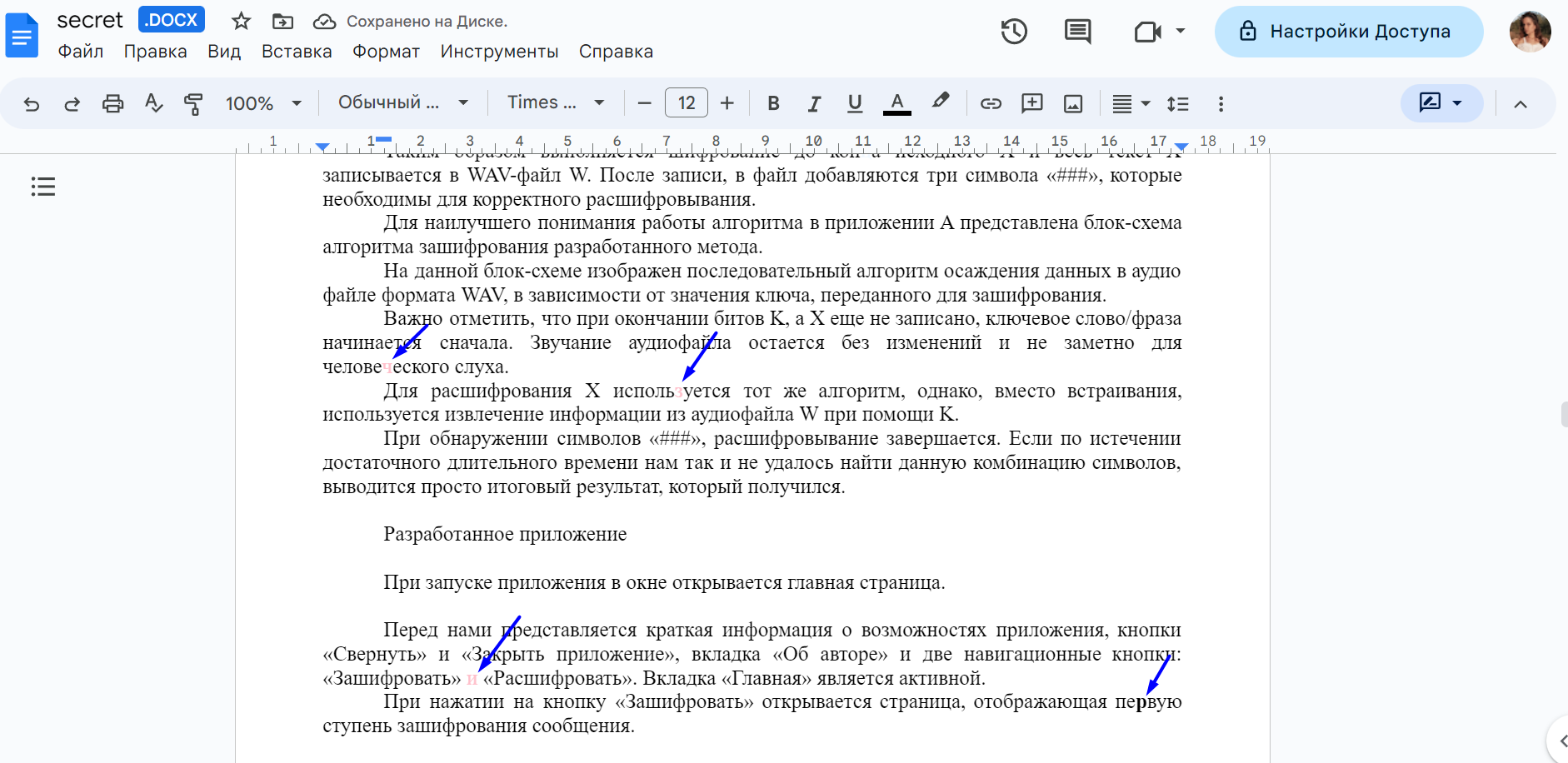


Рисунок 7 – Отображение намеренно измененных цветов символов для наглядного понимания

Пример данной программы, демонстрирующий метод апрош в текстовой стеганографии, раскрывает несколько ограничений и недостатков, которые снижают его надежность:

* Отсутствие шифрования приводит к уязвимости метода перед перехватом или вмешательством третьих лиц, поскольку скрытая информация остается незащищенной.
* Чувствительность к редактированию означает, что даже незначительные изменения в тексте-контейнере могут повлиять на скрытую информацию, что может затруднить ее извлечение или привести к ее повреждению.
* Ограниченный объем информации ограничивает количество данных, которые можно внедрить в текст. Это может быть недостаточно для передачи больших объемов информации или комплексных сообщений.

Использование метода апрош в текстовой стеганографии требует учета этих ограничений и недостатков, а также принятия мер для повышения безопасности и надежности метода, например, добавления шифрования или комбинирования с другими стеганографическими методами.

Вывод: в процессе выполнения лабораторной работы мы исследовали методы стеганографии, связанные с встраиванием и извлечением скрытой информации в электронные файлы текстового формата. Особое внимание было уделено методу, известному как Апрош, и разработано оконное приложение для наглядного демонстрирования его применения при шифровании и дешифровании данных.

Контрольные вопросы

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

Суть методов текстовой стеганографии заключается в скрытии секретной информации внутри текстового контейнера без вызывания подозрений у посторонних наблюдателей. Основная идея состоит в том, чтобы внедрить скрытую информацию в текст таким образом, чтобы изменения были незаметны для человеческого восприятия. При этом старается сохранить оригинальный внешний вид текста и его смысловую нагрузку.

Существует несколько методов текстовой стеганографии, и каждый из них использует свои подходы к сокрытию информации. Одним из распространенных методов является замена символов или слов в тексте на другие символы или слова, которые несут скрытую информацию. Другой метод заключается в использовании незаметных изменений в форматировании текста, таких как изменение размера шрифта, отступов, цветов и прочих атрибутов.

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

Методы синтаксической текстовой стеганографии основаны на изменении синтаксической структуры текста для внедрения скрытой информации. Вместо замены символов или слов, как в других методах стеганографии, синтаксическая стеганография модифицирует грамматическую структуру предложений или использует скрытые паттерны, чтобы внедрить данные.

*Метод синтаксической аномалии*

Данный метод основан на внедрении скрытых данных путем изменения грамматической структуры предложений таким образом, чтобы они стали аномальными с точки зрения обычной грамматики. Например, можно изменить порядок слов в предложении, добавить дополнительные слова или изменить их форму, чтобы закодировать скрытую информацию.

*Метод использования скрытых паттернов*

Этот метод использует определенные скрытые паттерны или шаблоны в тексте, которые могут быть использованы для кодирования данных. Например, можно использовать определенные комбинации слов или фраз, которые имеют скрытое значение или сигнализируют о наличии скрытой информации.

*Метод внедрения в структуру разделов или абзацев*

В этом методе скрытая информация внедряется в структуру разделов или абзацев текста. Например, можно использовать определенные разделы или абзацы для кодирования данных, задавая им специфическое значение или изменяя их порядок.

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

Методы лингвистической текстовой стеганографии основаны на использовании особенностей языка, лингвистических структур и свойств текста для внедрения скрытой информации. Эти методы включают в себя изменение слов, грамматики, семантики и других лингвистических аспектов текста.

*Метод замены синонимов*

В этом методе используются синонимы для замены определенных слов в тексте. Выбор синонимов может быть основан на заранее согласованном словаре или алгоритмическом подходе. Замена синонимов позволяет внедрить скрытую информацию, сохраняя общий смысл предложений.

*Метод изменения грамматики*

Данный метод изменяет грамматические структуры предложений для кодирования скрытой информации. Это может включать изменение порядка слов, использование других частей речи, внесение синтаксических изменений и т.д. Цель состоит в том, чтобы сделать изменения незаметными для обычного чтения, но передать скрытую информацию.

*Метод внедрения в семантику*

В этом методе скрытая информация внедряется в семантические аспекты текста. Это может быть использование определенных ключевых слов или фраз, которые имеют скрытое значение, а также изменение смысла определенных предложений или контекстуальной интерпретации текста.

Примером инструмента, реализующего методы лингвистической текстовой стеганографии, является "Linguistic Steganography Tool" (LST), который предлагает возможность внедрения скрытой информации в текст с использованием лингвистических подходов.

*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 их способности сохранить скрытую информацию и обеспечить ее незаметность в новом формате. Более стойкие методы успешно справляются с конвертацией и сохраняют скрытую информацию, минимизируя изменения в тексте и обеспечивая его нормальное восприятие.

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

Стеганографическая стойкость методов текстовой стеганографии при визуальном стеганоанализе текста-контейнера зависит от их способности скрыть наличие скрытой информации от наблюдателя. Более стойкие методы обеспечивают высокую невидимость внедрения и затрудняют обнаружение скрытой информации при визуальном анализе текста. Чем меньше различий между стеганографированным текстом и оригинальным текстом-контейнером, тем более стойким является метод.

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

Метод "χ-квадрат" является одним из распространенных методов стеганоанализа в области текстовой стеганографии. Он основывается на статистическом анализе распределения символов в тексте-контейнере для обнаружения наличия скрытой информации. При использовании метода "χ-квадрат" производится сравнение ожидаемой частоты появления символов с фактической частотой в тексте, и если есть значительные отклонения, то это может указывать на наличие скрытой информации. Метод "χ-квадрат" позволяет проводить статистический анализ и выявлять нерегулярности, которые могут быть связаны со внедрением скрытой информации в текст.

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

Апрош (Approach) - это метод или подход, используемый в контексте текстовой стеганографии. Он представляет собой определенную стратегию или способ реализации стеганометода.

Сущность стеганометода на основе модификации апроша заключается в изменении или доработке оригинального метода апроша с целью улучшения его характеристик, таких как стойкость, скрытность или незаметность. Модификация апроша может включать изменение алгоритмов внедрения и извлечения информации, использование дополнительных шифровальных методов, оптимизацию процессов или внедрение новых подходов к выбору места внедрения или характеристик символов.

Цель модификации апроша в стеганографии заключается в улучшении эффективности и стойкости метода, чтобы обеспечить более надежную и незаметную передачу скрытой информации. Модифицированный апрош может представлять собой оптимизированную версию оригинального метода или новый подход, основанный на его основных принципах, но с внесением дополнительных изменений и улучшений.

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

Кернинг - это процесс настройки промежутков между символами в типографском дизайне для достижения оптимального визуального равновесия и читаемости текста.

Сущность стеганометода на основе модификации кернинга заключается в использовании изменения промежутков между символами в тексте как способа внедрения скрытой информации. При такой модификации кернинга в тексте-контейнере определенные промежутки между символами изменяются согласно битовой последовательности скрытой информации. Таким образом, выбранные промежутки между символами служат для кодирования скрытого сообщения.

Стеганометод на основе модификации кернинга может быть использован в текстовой стеганографии для скрытной передачи информации, обеспечивая незаметность изменений для наблюдателя. Поскольку изменения касаются только промежутков между символами, визуальное восприятие текста остается почти неизменным, что облегчает скрытное внедрение и извлечение информации.