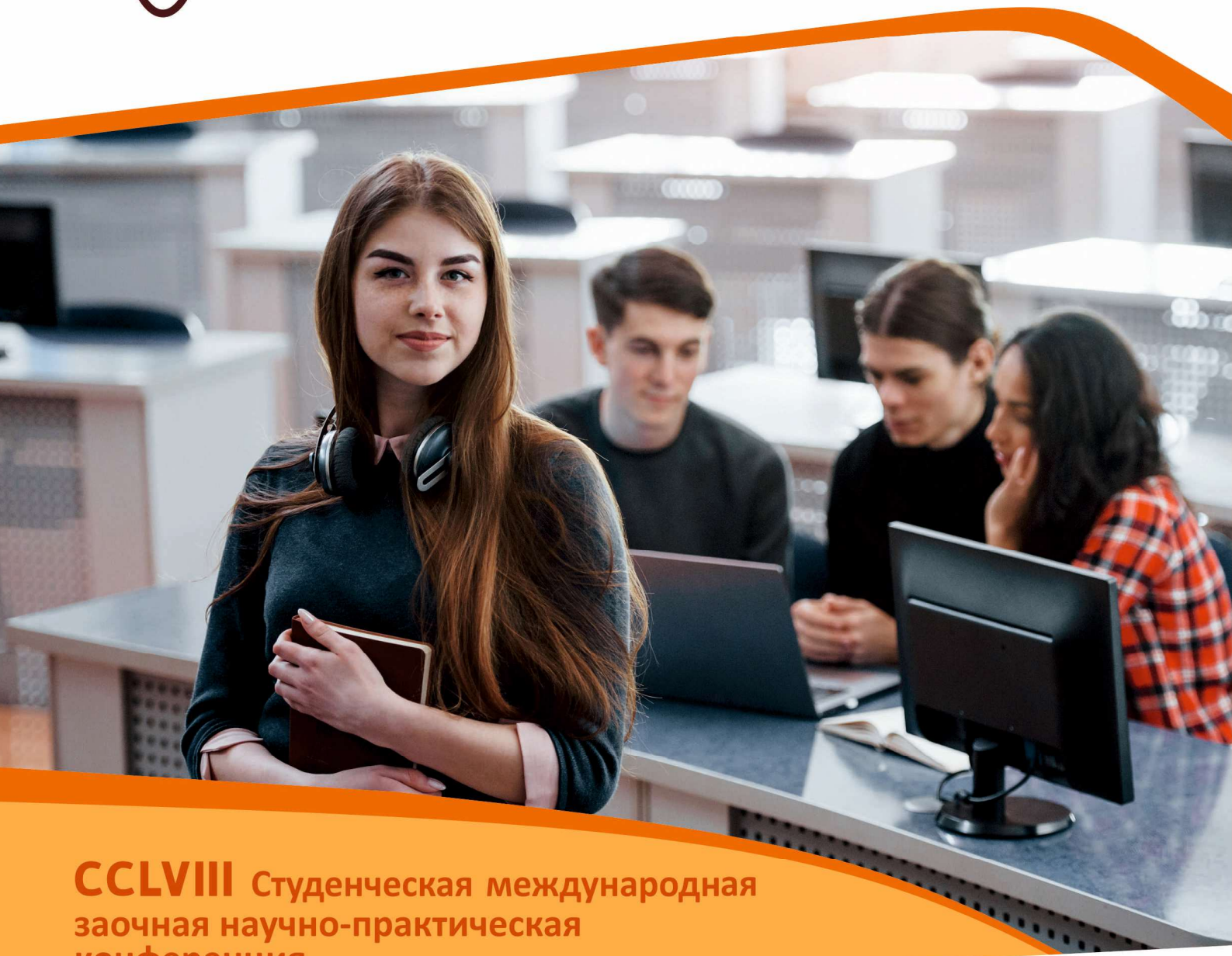
НАУЧНЫЙ ФОРУМ
nauchforum.ru

ISSN 2618-6829



CCLVIII Студенческая международная заочная научно-практическая конференция

МОЛОДЕЖНЫЙ НАУЧНЫЙ ФОРУМ

№26(258)

г. МОСКВА, 2024

МОЛОДЕЖНЫЙ НАУЧНЫЙ ФОРУМ

Электронный сборник статей по материалам CCLVIII студенческой международной научно-практической конференции

№ 26 (258)
Июль 2024 г.

Издается с декабря 2017 года

Москва
2024

УДК 08
ББК 94
М75

М75 Молодежный научный форум. Электронный сборник статей по материалам CCLVIII студенческой международной научно-практической конференции. – Москва: Изд. «МЦНО». – 2024. – №26 (258) / [Электронный ресурс] – Режим доступа. – URL: https://nauchforum.ru/archive/MNF_interdisciplinarity/26(258).pdf

Электронный сборник статей CCLVIII студенческой международной научно-практической конференции «Молодежный научный форум» отражает результаты научных исследований, проведенных представителями различных школ и направлений современной науки.

Данное издание будет полезно магистрам, студентам, исследователям и всем интересующимся актуальным состоянием и тенденциями развития современной науки.

ББК 30+22.1
ISSN 2618-6829

Оглавление

РУБРИКА 1.

«ТЕХНИЧЕСКИЕ НАУКИ»

ПРИМЕНЕНИЕ ПРОГРАММЫ STEGANPEG ДЛЯ СОКРЫТИЯ ИНФОРМАЦИИ НА ОСНОВЕ МЕТОДА НЗБ

Баталин Ярослав Леонидович
студент,
Санкт-Петербургский государственный университет
Телекоммуникаций им. профессора М.А. Бонч-Бруевича,
РФ, г. Санкт-Петербург

USING THE STEGANPEG PROGRAM TO CONCEAL INFORMATION BASED ON THE LSB METHOD

Yaroslav Batalin
Student,
St. Petersburg State University
of Telecommunications
named after Professor M.A. Bonch-Bruevich,
Russia, St. Petersburg

Аннотация. в статье представлено применение стеганографических методов встраивания информации в изображения с помощью программы SteganPEG. Данная программа позволяет скрывать информацию в изображениях

Abstract. The article presents the application of steganographic methods for embedding information into images using the SteganPEG program. This program allows you to hide information in images

Ключевые слова: Стеганография, стеганографические методы, сокрытие информации, LSB, НЗБ, SteganPEG.

Keywords: Steganography, steganographic methods, information concealment, LSB, SteganPEG.

Цель исследования: проанализировать возможные преимущества и недостатки сокрытия информации с помощью программы SteganPEG.

Введение. Термин стеганография в широком смысле означает «скрытие» или покрытие информации. С момента появления информации и способности обмениваться ею возникла потребность в сокрытии этой информации от третьих лиц. Современная стеганография (цифровая стеганография) делится на две взаимосвязанные, но различающиеся по целям использования части:

1. Собственно стеганография (СГ)**: Основной целью является такое преобразование основной информации в стеганограмму, которое делает факт присутствия дополнительной информации незаметным или, по крайней мере, затруднительным для обнаружения нелегитимными пользователями.

2. Цифровые водяные знаки (ЦВЗ)**: Целью систем ЦВЗ является скрытное (или иногда открытое) встраивание дополнительной информации в контент, обеспечивающее высокое качество исходного объекта после встраивания и исключающее возможность удаления водяного знака нелегитимными пользователями. Основное применение ЦВЗ – защита прав собственности на аудио, видео, текстовые объекты и программные коды.

Существует несколько видов стеганографии, среди которых можно выделить:

- Текстовая стеганография: Встраивание информации в текстовые документы.
- Стеганография в неподвижных изображениях: Встраивание информации в графические файлы.
- Стеганография в подвижных изображениях: Встраивание информации в видеофайлы.
- Стеганография в звуке: Встраивание информации в аудиосигналы.
- Стеганография в интернет-протоколах: Встраивание информации в данные, передаваемые через интернет-протоколы.

Рассмотрим один из видов стеганографии – метод наименьшего значащего бита (LSB, Least Significant Bit). Этот метод является одним из наиболее простых и широко используемых для скрытия информации в цифровых изображениях. В

LSB данные внедряются в наименьшие значащие биты пикселей изображения, что позволяет скрыть информацию, не заметно изменяя визуальное качество изображения.

Алгоритм:

1. Преобразование данных в двоичный формат: Преобразование секретных данных (например, текста) в двоичное представление.

2. Извлечение пикселей из изображения: Представление изображения как матрицу пикселей, где каждый пиксель имеет цветовые компоненты (например, R, G, B).

3. Внедрение данных: Последовательная замена наименьшего значащего бита каждой цветовой компоненты пикселя на очередной бит секретных данных.

4. Сохранение стеганографического изображения: Сохранение измененной матрицы пикселей как новое изображение

На рис.1 представлена формула, по которой происходит работы алгоритма.

$$C_w(n) = \sum_{i=1}^{L-1} c_i(n) 2^i + b(n)$$

Рис. 1. Формула замены наименьшего значащего бита

Где b(n) – биты вкладываемой информации;

L – длина битовой последовательности;

$C_i(n)$ – двоичные коэффициенты;

Инструкция по установке ПО:

Сначала необходимо перейти по данной ссылке. После чего нужно нажать на кнопку «Скачать Бесплатно» на рис. 2 представлено внешнее оформление сайта

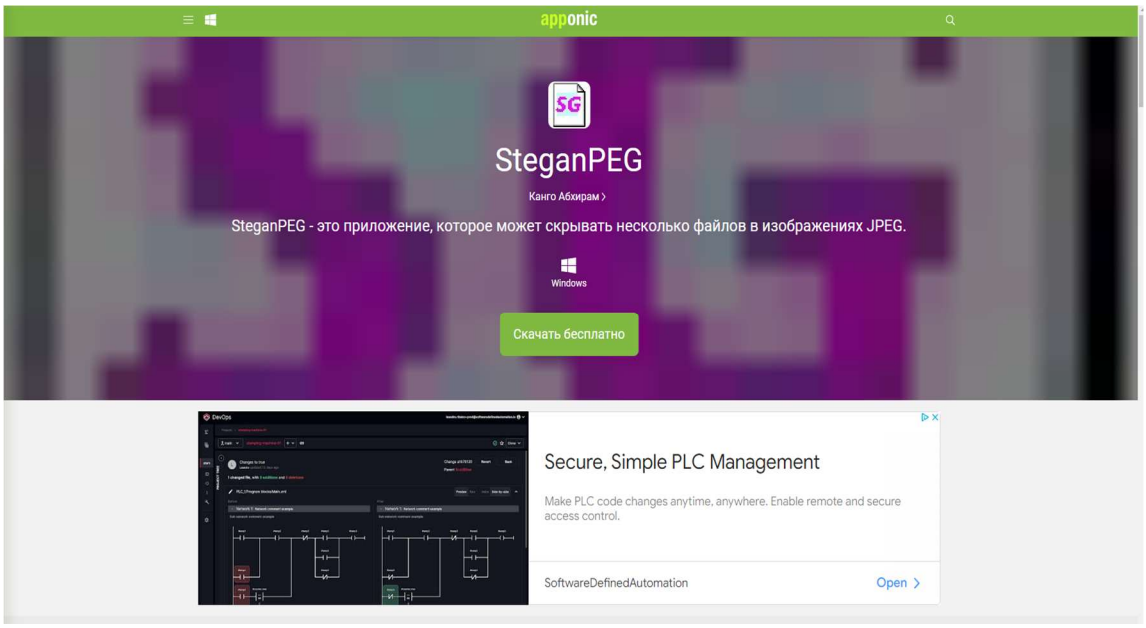


Рисунок 2. Оформление сайта

После выполнения первого шага, необходимо открыть скаченный архив. Пример архива приведен на рис.3.

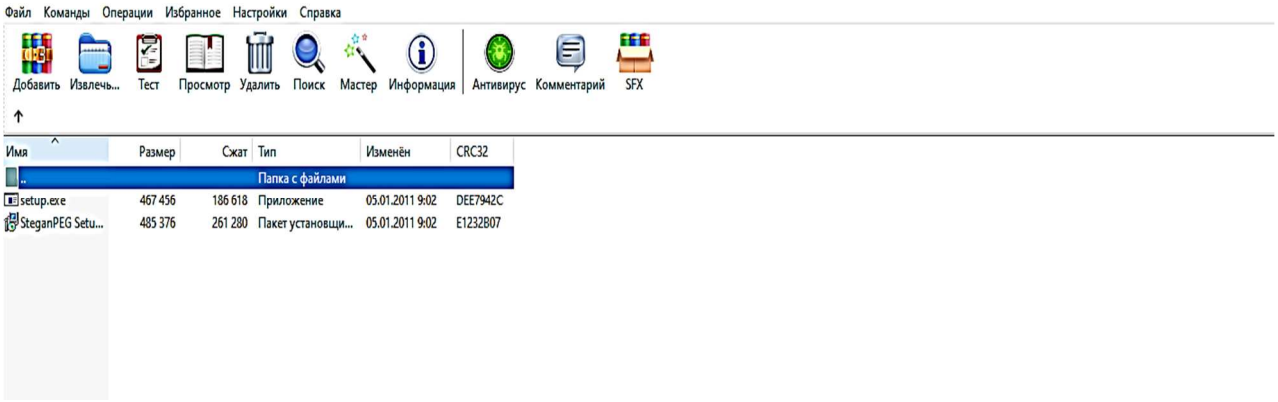


Рисунок 3. Скаченный архив

Далее необходимо открыть файл setup.exe и пройти процесс установки. При удачной инсталляции приложения появится окно, представленное на рис.4

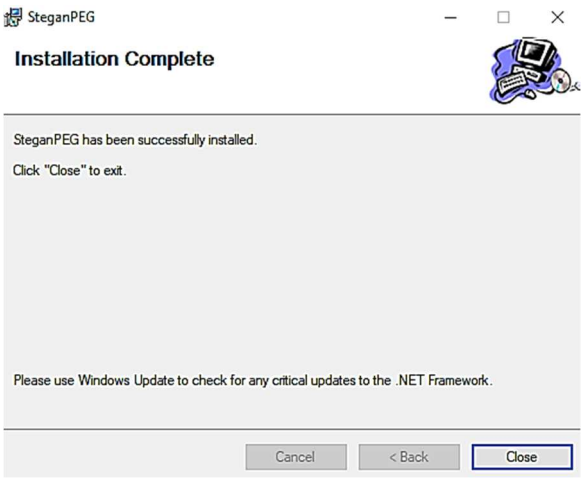


Рисунок 4. Окно удачной инсталляции приложения

Описание работы программы:

Для того, чтобы скрыть информацию, необходимо любое изображение формата JPEG и TXT файл, в котором будет написана информация для сокрытия. Далее необходимо в интерфейсе программы представленном на рис.5, в пункте «Please choose an action to perform» выбрать «Embed files into a JPEG image», после чего необходимо ввести пароль в графе «Enter a password to encrypt the files in the image», который будет использован в дальнейшем для извлечения информации. А также в пункте «Enter path to image file» выбрать файл формата JPEG в котором будет скрыта информация. После выполнения всех действий необходимо нажать на кнопку «Go!»

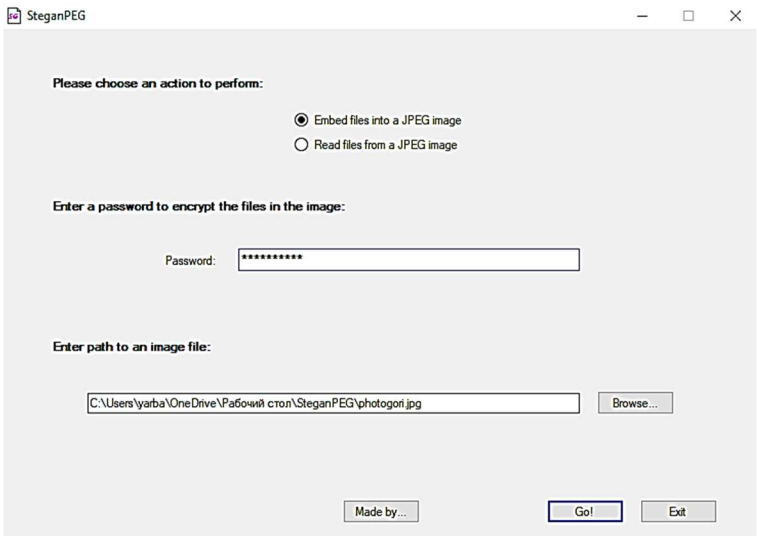


Рисунок 5. Интерфейс программы SteganPEG

В следующем окне программы, представленном на рис.6, необходимо выбрать txt файл, нажав на кнопку «Add file». Так же есть ограничение по весу txt файла, оно показано в графе «image space occupied» в случае, если места будет недостаточно, вам необходимо выбрать другой JPEG файл с большим количеством пикселей. После добавления файла, необходимо нажать на кнопку «Save Stegged image». Файл со скрытым txt файлом сохранится в тоже директории, что и оригинальный.

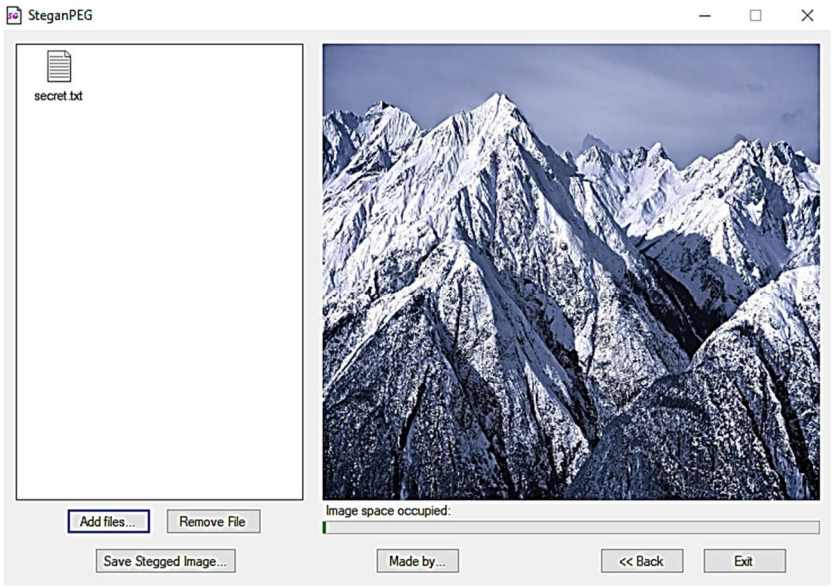


Рисунок 6. интерфейс выбора скрываемого файла.

На рис.7 и рис.8 представлены начальное изображение и результат внедрения текстовых данных в файл контейнер

Рисунок 7. Начальное изображение

Рисунок 8. Результат внедрения

Что бы извлечь данные из файла-контейнера, необходимо открыть программу SteganPEG, в пункте «Please choose an action to perform» выбрать «Read files into a JPEG image», после чего необходимо ввести пароль в графе «Enter a password to encrypt the files in the image», который был использован ранее, при сокрытии информации. А также в пункте «Enter path to image file» выбрать файл формата JPEG который был получен при сокрытии информации. После выполнения всех действий необходимо нажать на кнопку «Go!». Интерфейс программы для извлечения данных представлен на рис.9.

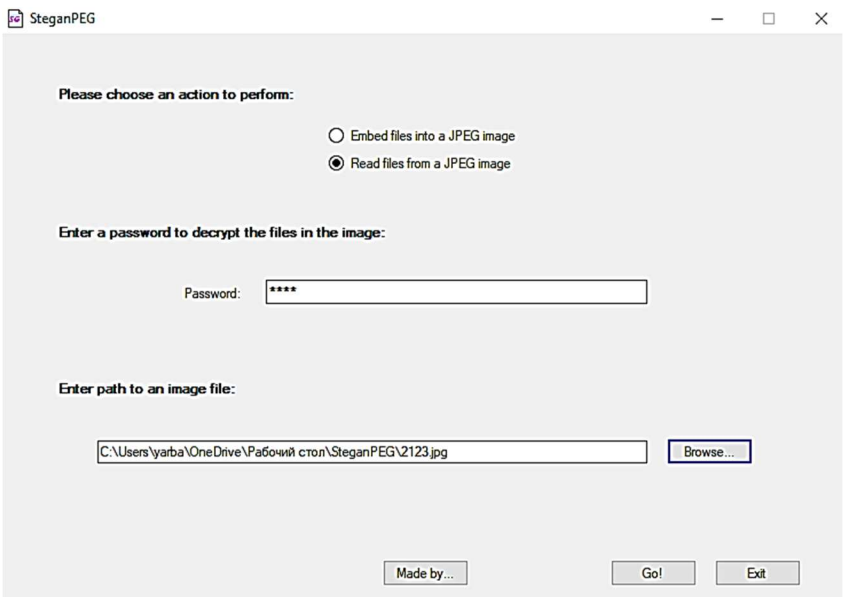


Рисунок 9. Интерфейс программы для извлечения данных

Далее в следующем окне необходимо при помощи левой кнопки мыши выбрать файлы, которые вы хотите извлечь и нажать на копку «Save selected» и выбрать директорию для сохранения. Интерфейс программы представлен на рис.10.

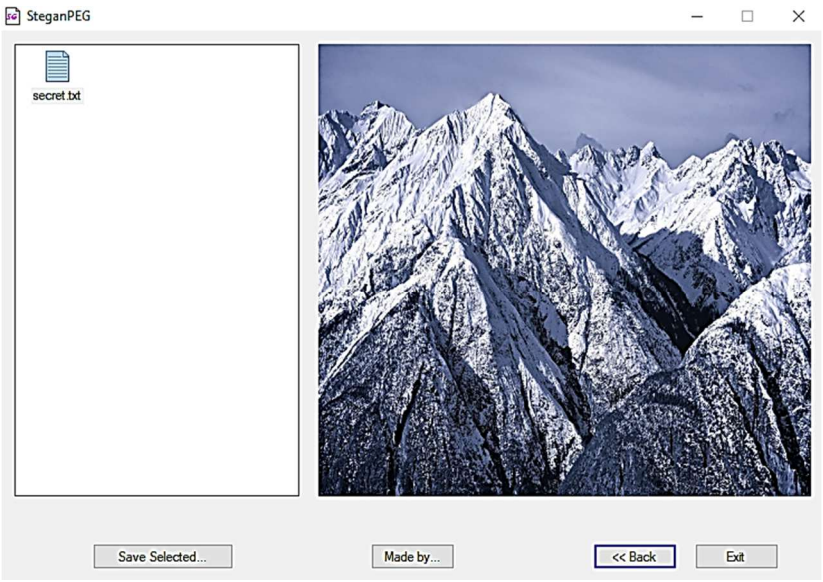


Рисунок 10. Извлечение файлов

При успешном извлечении файлов появится окно, продемонстрированное на рис.11.

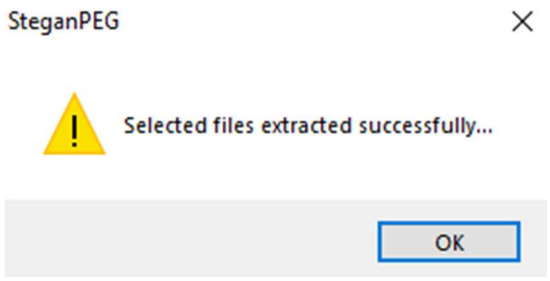


Рисунок 11. Успешное извлечение файлов

Принцип работы программы SteganPEG

Программа SteganPEG предназначена для скрытия информации в цифровых изображениях с использованием метода стеганографии на основе наименьших значащих бит (LSB). Вот основные принципы её работы:

1. **Выбор изображения:** Пользователь выбирает цифровое изображение, в которое будет внедряться скрытая информация. Это может быть любой формат изображения, поддерживаемый программой.

2. **Преобразование данных:** Секретные данные, которые нужно скрыть, преобразуются в битовый формат. Например, текстовые данные переводятся в последовательность битов.

3. **Внедрение данных в изображение:**

- Каждый пиксель изображения рассматривается как набор цветовых компонент (например, RGB для цветных изображений).
- Для каждого пикселя выбираются наименьшие значащие биты (LSB) каждой цветовой компоненты.
- Биты скрытой информации последовательно встраиваются в эти наименьшие значащие биты пикселей изображения.
- Это позволяет сохранить визуальное качество изображения, так как изменения в наименьших значащих битах обычно незаметны для человеческого глаза.

4. **Сохранение стеганографического изображения:** Измененное изображение, содержащее скрытую информацию, сохраняется в новый файл. Этот файл может быть визуально неразличим от оригинала, но в нем содержится дополнительная скрытая информация.

Вывод: SteganPEG- мощная и удобная программа для стеганографии, предоставляющая множество функций для безопасного сокрытия данных, оснащенная простым и интуитивно понятным интерфейсом

Список литературы:

1. Коржик, В.И. Цифровая стеганография : учебник / В.И. Коржик, А.В. Красов. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2023. – 324 с. – ISBN 978-5-406-10970-0. – EDN KNKBXU.
2. Коржик, В.И. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения / В.И. Коржик, З.К. Нгуен, А.В. Даньшина // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13, № 5. – С. 75-85. – EDN COUQRN.

3. 21 лучший инструмент для обеспечения безопасности ваших данных [Электронный ресурс]. URL: https://technicalustad.com/steganography-tools/ (дата обращения 12.07.2024)
4. Коржик В.И., Нгуен З.К., Даньшина А.В. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения. Том 13 – Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия: научная статья, 2021, 75-85 с, ISSN: 2409-5419
5. Цифровая стеганография и цифровые водяные знаки / В.И. Коржик, К.А. Небаева, Е.Ю. Герлинг [и др.] ; Под общей редакцией профессора В.И. Коржика. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – 226 с. – ISBN 978-5-89160-125-3. – EDN WJYYGJ.

ЭФФЕКТИВНОЕ СОКРЫТИЕ ДАННЫХ ПРИ ПОМОЩИ STEGANO: РУКОВОДСТВО И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Конторов Владимир Федорович
студент,
Санкт-Петербургский государственный университет
Телекоммуникаций им. профессора М.А. Бонч-Бруевича
Большевиков,
РФ г. Санкт-Петербург

EFFICIENT DATA HIDING USING STEGANO: GUIDELINES AND INFORMATION SECURITY METHODS

Vladimir Kontorov
студент,
St. Petersburg State University of Telecommunications
named after. Professor M.A. Bonch-Bruevich
Russia, St. Petersburg

Аннотация. В статье приведено руководство по использованию библиотеки stegano, которая используются для сокрытия информации при помощи метода LSB, использования красной части пикселя для скрытия ASCII-сообщений. Подробно описаны действия, которые необходимо предпринять, чтобы сокрыть и/или извлечь информацию при помощи данной библиотеки, помимо этого рассмотрены ситуации, в которых зашифрованная информация становится нечитаемой, и варианты решения данной проблемы.

Abstract. The article provides guidance on using the stegano library, which is used to hide information using the LSB method, using the red part of the pixel to hide ASCII messages. The actions that need to be taken to hide and/or extract information using this library are described in detail, situations in which encrypted information becomes unreadable, and options for solving this problem are also considered.

Ключевые слова: стеганография, stegano, метод наименьшего значащего бита(LSB), статистический стег-анализ, стег-анализ LSB-кодирования в цветных изображениях.

Keywords: steganography, stegano, least significant bit (LSB) method, statistical steganalysis, steganalysis of LSB coding in color images.

Стеганография - это наука о скрытой передаче информации. Она остается актуальной в современном мире по нескольким причинам. Во-первых, стеганография позволяет скрывать сам факт существования информации, что делает ее более эффективной и менее подверженной обнаружению, чем криптографические методы. Во-вторых, с развитием цифровых технологий и интернета появляются новые возможности для применения стеганографии, так как данные можно легко скрывать в различных мультимедийных файлах.

Кроме того, стеганография также находит применение в сфере цифрового маркетинга и защите авторских прав. Например, она может использоваться для встраивания скрытой информации в изображения или видео, что позволяет создавать водяные знаки или автоматически отслеживать распространение контента в сети. В сфере кибербезопасности стеганография может помочь в предотвращении утечек конфиденциальной информации и защите данных от нежелательного доступа. Путем скрытой передачи информации стеганография позволяет предотвратить обнаружение и перехват данных злоумышленниками, что повышает уровень безопасности коммуникаций и информационных систем. Таким образом, стеганография остается актуальной и востребованной в различных областях, где необходимо обеспечить конфиденциальность и надежность передачи информации. Ее возможности и преимущества делают ее эффективным инструментом для работы с секретной информацией и обеспечения безопасности данных в цифровой среде. В нашей статье мы рассмотрим пользовательскую библиотеку stegano (Python), созданную следущими людьми в 2010 году:

Седрик Боном, Адриен Коссон, Эндрю Робертс, Кристоф Гессен, Флавьен Ру, Максвелл Гербер,Nejdet Çağdaş Yücesoy, Панни, Питер Джастин, Thundersparkf.

С помощью stegano можно написать код на языке Python, который посредством метода LSB сможет спрятать некоторое сообщение в файле формата png, jpg, а также извлечь вложенное сообщение.

Существует несколько основных методов стеганографии, которые используются для скрытой передачи информации:

Метод наименьшего значащего бита (Least Significant Bit, LSB): это один из наиболее распространенных методов стеганографии, при котором информация скрывается в младших битах пикселей изображения или звуковых сэмплов. Этот метод позволяет сохранять визуальное или звуковое качество носителя, при этом скрываемая информация остается незаметной для человеческого восприятия.

Метод Фейстеля: этот метод основан на использовании алгоритма шифрования Фейстеля для встраивания информации в носитель. Данные разбиваются на блоки и шифруются с использованием ключа, после чего информация встраивается в зашифрованные блоки. Этот метод обеспечивает дополнительный уровень безопасности за счет использования шифрования.

Маскировка вносимых изменений: данный метод предполагает встраивание информации в носитель путем изменения его статистических характеристик. Например, это может быть изменение статистики цветовых значений пикселей изображения или характеристик аудиофайлов. Этот подход позволяет скрыть наличие скрытой информации от обнаружения.

Преобразование методом встроения: этот метод основан на преобразовании содержимого носителя для встраивания информации, например, путем изменения последовательности пикселей изображения или добавления "шума" в аудиосигнал. Такие изменения вносятся таким образом, чтобы скрытая информация сохраняла свою целостность и оставалась неотличимой от исходного носителя.

Нас интересует в первую очередь метод наименьшего значащего бита, поскольку именно он реализован в библиотеке stegano.

В 17 веке Го́тфрид Ви́льгельм Ле́йбниц описал двоичную систему счисления и заложил основы математической логики, в 1948 году Клод Э́лвуд Ше́ннон написал статью «Математическая теория связи», в которой высказал идею,

заключающуюся в том что сообщения могут иметь некоторое «значение». Помимо этого он начал рассматривать непрерывные множества сообщений, а не только конечные. Эта статья позволила решить основные задачи теории информации: кодирование, передачу сообщений и устранение избыточности.

Что собственно в итоге и привело к появлению множества стеганографических методов, в том числе и поспособствовало появлению метода наименьшего значащего бита.

LSB работает следующим образом, он изменяет младшие биты в байтах, которые отвечают за кодирование цвета. Предположим, что в нашем сообщении есть байт 11011000, а байты в изображении –…10101111 01101101 01111110 1101100100…, то кодирование будет выглядеть так. Мы разобьем байт секретного сообщения на 4 двухбитовые части: 11, 01, 10, 00, и заменим ими младшие биты изображения: …10101111 01101101 01111110 1101100100…. В результате получается оттенок, который будет очень похож на изначальный. Эти цвета трудно различить даже на большой по площади заливке, хотя разница будет заметна по одному отдельному пикселю. Практика показывает, что замена двух младших битов не воспринимается человеческим глазом. В случае необходимости можно занять и три бита, что весьма незначительно скажется на качестве картинки. Большее количество будет уже более заметно, что сделает использование данного метода бесполезным, в результате, если использовать два бита из восьми на каждый канал, то имеется возможность скрыть до трех байт информации на каждые четыре пикселя изображения, что соответствует четверти от объема картинки. Таким образом, имея файл изображения размером 100 Кбайт, можно скрыть в нем до 25 Кбайт полезных данных так, что человеческий глаз не сможет заметить изменений в изображении.

К преимуществам данного метода можно отнести то, что младшие биты изображений могут иметь различное распределение зависящее от применяемых параметров аналого-цифрового преобразования, от дополнительной компьютерной обработки и от прочих факторов. Эта особенность делает метод наименее значащих битов наиболее защищенным от обнаружения вложения. Также реализация метода

LSB для большинства стандартов файлов-контейнеров не требуют значительных затрат времени и сил.

Метод LSB, несмотря на свою простоту, имеет один существенный недостаток: информация, скрытая этим методом, легко обнаруживается. Задача обнаружения обычно решается методами статистического анализа. Например, если мы хотим скрыть некоторый фрагмент текстового сообщения, это сообщение будет содержать только символьную информацию: 66 знаков кириллицы, 52 знака латиницы, знаки препинания и некоторые служебные символы. Если сравнить статистические характеристики такого сообщения и статистические характеристики младших битов красного спектра, то будут видны существенные отличия. Это обусловлено тем, что последовательность последних битов красного спектра представляет из себя случайную двоичную последовательность, а наше сообщение не является такой последовательностью.

Перейдем собственно к библиотеке stegano, на изображениях 1 и 2 вы можете наблюдать изначальное изображение и изображение с вложенным сообщением соответственно, оба изображения изначально в формате png:

Рисунок 1. изображение 1 (без вложенного сообщения), изображение 2 (с вложенным сообщением)

в данном случае размер изображения после вложения информации увеличился почти в 7 раз, при сжатии изображения скрытую часть извлечь не получается, так

же как и при повороте изображения, к изменению же формата файл оказался устойчив.

На изображениях 3 и 4 вы можете наблюдать изначальное изображение и изображение с вложенным сообщением соответственно, оба изображения изначально в формате jpg:

Рисунок 2. Изображение 3(без вложенного сообщения)

Рисунок 3. Изображение 4(с вложенным сообщением)

в данном случае размер изображения с вложенным сообщением оказался полтора раза меньше размера изображения без скрытого сообщения, сжатие данное изображение также не пережило, но в отличие от первого изображения, из второго можно извлечь информацию при повороте, к переименованию изображение номер два также оказалось устойчиво.

Подводя итоги хочется сказать, что stegano достаточно удобный инструмент, для пользования которым не требуется прилагать никаких усилий, но в тоже

время информация скрытая при помощи данной библиотеки не особо устойчива к изменениям изображений, а так же легко обнаруживается, что делает ее не особо востребованной в профессиональной деятельности

Список литературы:

1. Красов, А.В. Модель нарушителя информационной безопасности, использующего стеганографические каналы взаимодействия / А.В. Красов // Наука и бизнес: пути развития. – 2022. – № 4(130). – С. 79-88. – EDN TZAHFJ.
2. Официальный сайт stegano URL: https://stegano.readthedocs.io
3. Коржик, В.И. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения / В.И. Коржик, З.К. Нгуен, А.В. Даньшина // Наукоемкие технологии в космических исследованиях Земли. – 2021. – Т. 13, № 5. – С. 75-85. – EDN COUQRN.
4. Красов, А.В. Использование методов машинного обучения при выявлении сетевой стеганографии / А.В. Красов, Н.В. Паскидов, А.С. Салита // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. – 2022. – № 3. – С. 50-53. – DOI 10.46418/2079-8199_2022_3_7. – EDN SBTDPU.
5. Коржик, В.И. Цифровая стеганография : учебник / В.И. Коржик, А.В. Красов. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2023. – 324 с. – ISBN 978-5-406-10970-0. – EDN KNKBXU.

ИСПОЛЬЗОВАНИЕ DEEPSOUND ДЛЯ РЕАЛИЗАЦИИ СКРЫТЫХ СТЕГАНОГРАФИЧЕСКИХ КАНАЛОВ ВЗАИМОДЕЙСТВИЯ

Коркин Андрей Семенович
студент,
Санкт-Петербургский государственный
университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича
РФ, г. Санкт-Петербург

USING DEEPSOUND TO IMPLEMENT HIDDEN STEGANOGRAPHIC INTERACTION SIGNALS

Andrey Korkin
Student,
The Bonch-Bruevich Saint-Peterburg
State University of Telecommunications
Prospekt Bolshevikov,
Russia, St. Petersburg

Аннотация. Утилита DeepSound, используемая в стеганографии, позволяет скрывать информацию в цифровых аудиофайлах. Она работает следующим образом: Пользователи могут встраивать секретные сообщения, изображения или другие файлы в аудиофайл, не изменяя его воспринимаемого звучания.

Abstract. The Deepsound utility, used in steganography, allows you to hide information in digital audio files. It works like this: Users can customize secret messages, images, or other files in an audio file without changing how it sounds**.**

Ключевые слова: стеганография, стеганографические методы, сокрытие информации, LSB, Deepsound.

Keywords: steganography, steganographic methods, information hiding, LSB, Deepsound.

Deepsound остается актуальным инструментом в стеганографии благодаря своим передовым алгоритмам и надежным возможностям сокрытия информации.

В эпоху цифровых данных стеганография становится все более важной для защиты конфиденциальной информации.

Стеганография – это практика сокрытия сообщений или данных внутри другого сообщения или файла таким образом, чтобы их нельзя было обнаружить. Она отличается от шифрования, которое делает данные нечитаемыми, но не скрывает их существование.

Метод извлечения информации: Получатели могут извлечь скрытую информацию из аудиофайла, используя ту же утилиту Deepsound и секретный ключ. Deepsound использует передовые алгоритмы для обеспечения надежного скрытия информации, что делает ее ценным инструментом для стеганографии.

Цель исследования: проанализировать возможности, преимущества и недостатки сокрытия информации через утилиту Deepsound

Основная часть:

Инструкция по установке ПО:

Для начала нам нужно установить саму программу для Windows, для этого переходим по этой ссылке: https://deepsound.ru.uptodown.com/windows

Сама иконка ПО. Нажимаем и открывается само меню DeepSound.

Описание работы ПО:

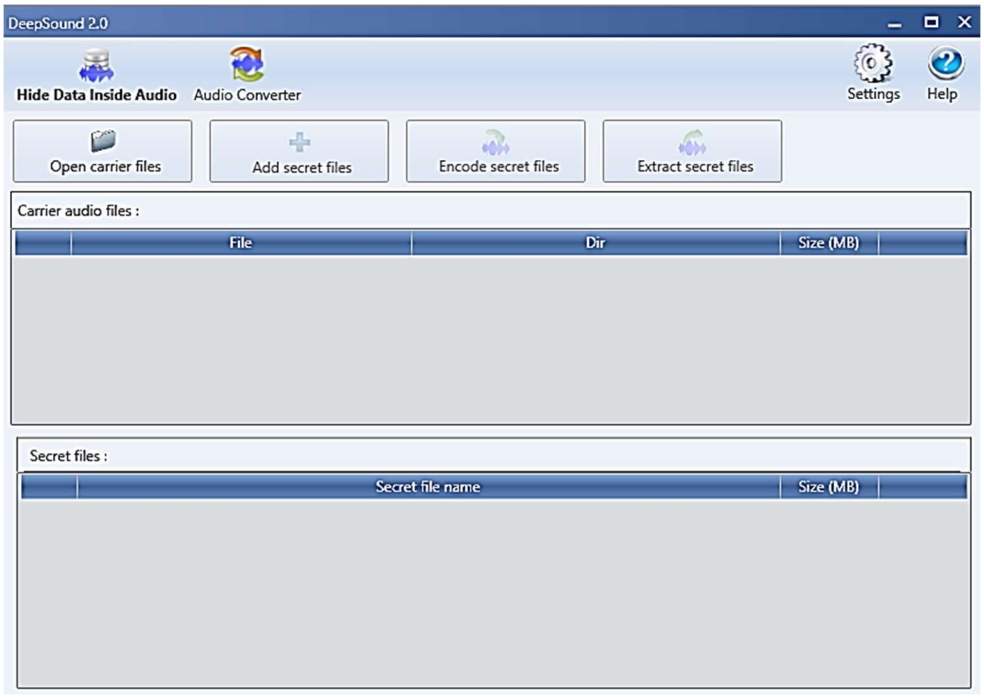


Рисунок 1. Пример

Здесь представлен весь функционал нашего приложения, через который можно сокрыть информацию, создав пароль для приложения, скрыв от посторонних сам факт передачи информации.

Рисунок 2. Пример

Данная кнопка отвечает за сам функционал сокрытия информации в другом файле.

Нажимая «Hide Data Inside Audio» появляется интерфейс, в котором можно указать файл, в котором нужно спрятать информацию, и можно указать информацию, которая будет храниться внутри этого файла.

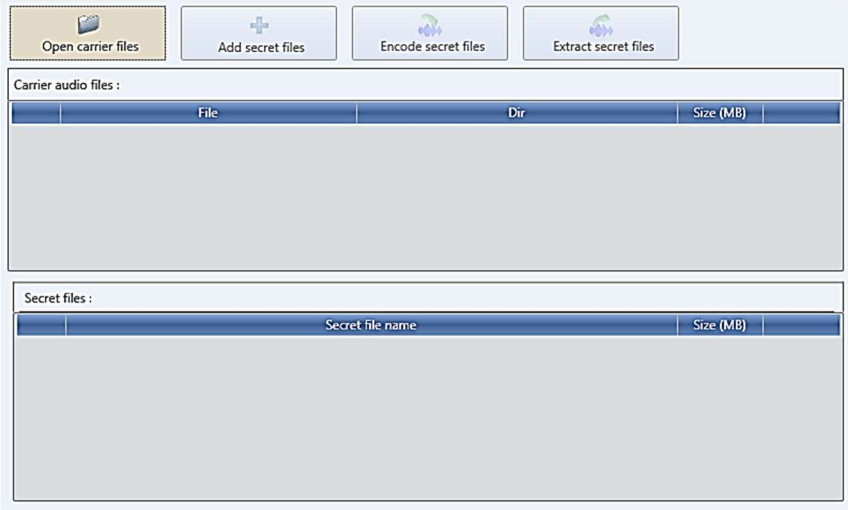


Рисунок 3. Пример

Для начала нужно добавить файл, в котором мы спрячем информацию, для этого нажимаем кнопку «Open carrier files», после этого кнопка «Add secret files» станет доступной.

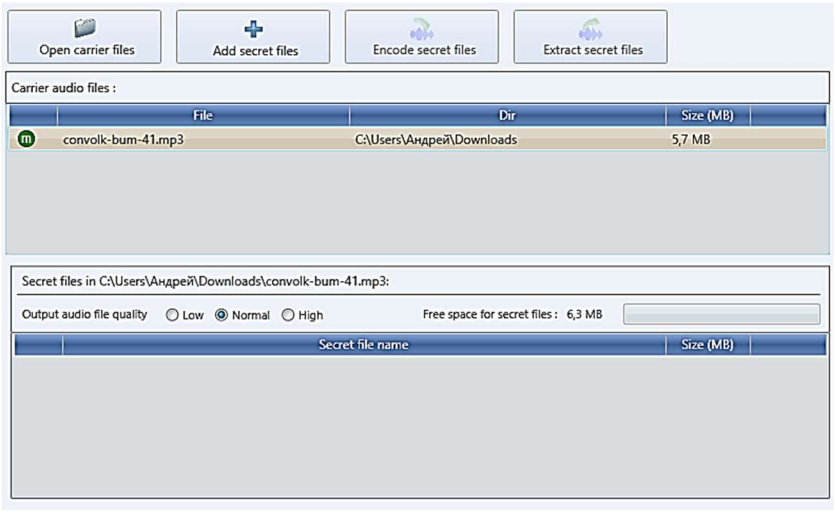


Рисунок 4. Пример

После чего мы нажимаем «Add secret files», добавляя любой файл, который мы хотим скрыть от пользователей.

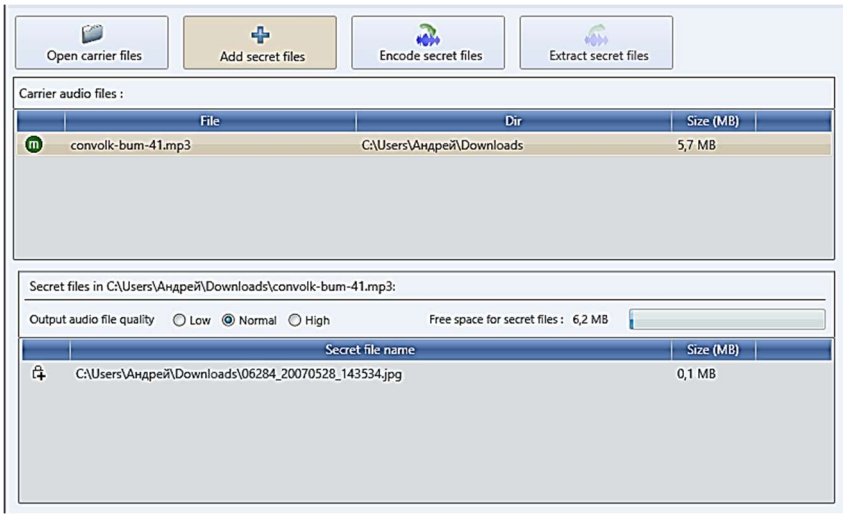


Рисунок 5. Пример

После этого нажимаем кнопку «Encode secret files», после чего наш файл будет готов, и информация в нём будет сохранена.

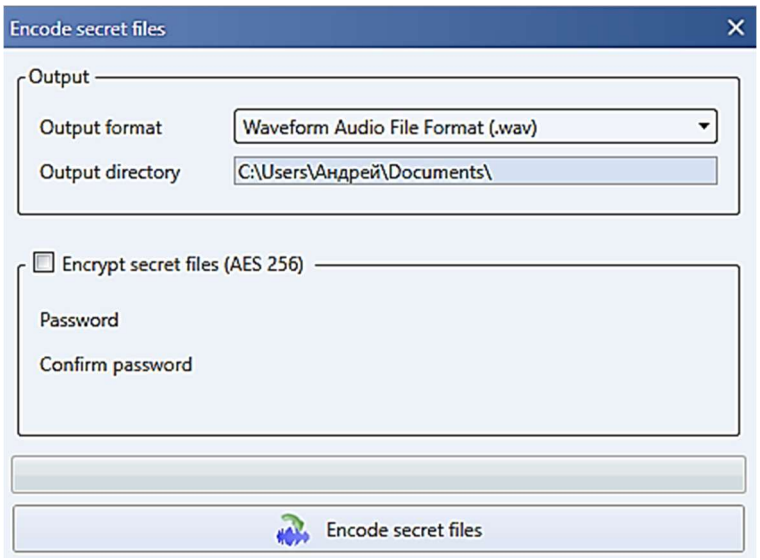


Рисунок 6. Пример

Так же можно добавить пароль для того чтобы открыть секретный файл, путём использования DeepSound.

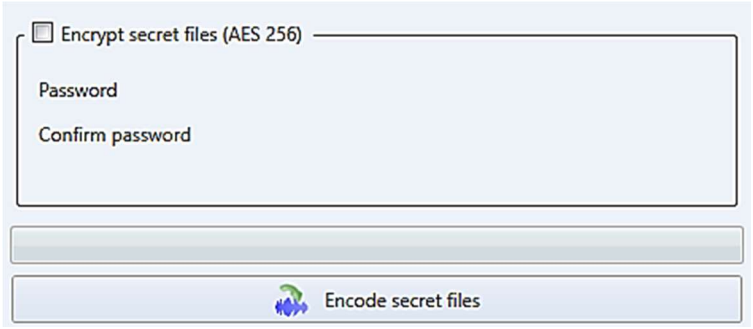


Рисунок 7. Пример

Добавить можно любой пароль, используя и латиницу, и кириллицу. Так же можно использовать любые знаки и цифры. Всё будет сохранено путем кодирования файла через AES 256.

DeepSound использует глубокие нейронные сети для обнаружения скрытых сообщений в аудиосигналах. Архитектура нейронной сети обычно состоит из нескольких сверточных слоев, за которыми следуют полностью связанные слои.

Сверточные слои извлекают локальные характеристики из аудиосигнала с помощью сверточных фильтров. Каждый фильтр представляет собой небольшую

матрицу, которая скользит по аудиосигналу, вычисляя свертку между фильтром и сигналом.

Выход сверточного слоя представляет собой карту признаков, которая содержит информацию о наличии скрытых сообщений. Полностью связанные слои объединяют характеристики, извлеченные сверточными слоями, и используют их для классификации аудиосигнала как содержащего или не содержащего скрытое сообщение. Выход полностью связанного слоя представляет собой вероятность того, что аудиосигнал содержит скрытое сообщение.

Математически НЗБ определяется следующим образом:

$$W(a, b) = \int_{-\infty}^{\infty} x(t) \psi_{a, b}(t) dt$$

где: `W(a, b)` - вейвлет-преобразование x(t) - звуковой сигнал `\psi_{a, b}(t)` - вейвлет-функция

DeepSound разработан исследователями из Технического университета Дармштадта в Германии. DeepSound позволяет обнаруживать скрытые сообщения, внедренные в аудиосигналы с помощью стеганографических методов. Он работает с различными форматами аудиофайлов и может использоваться в различных операционных системах. Данное ПО доступно для следующих операционных систем: Windows, macOS и Linux.

Форматы входных файлов: WAV, MP3, FLAC, OGG и AAC. DeepSound не создает выходных файлов. Он предоставляет оценку вероятности того, что аудиофайл содержит скрытое сообщение. Эта оценка может быть сохранена в текстовом файле или выведена на экран.

Первая версия DeepSound была выпущена в 2019 году и представлена на конференции ACM по компьютерной и коммуникационной безопасности (CCS). С тех пор DeepSound постоянно развивается и обновляется. В качестве контейнеров DeepSound может использовать WAV (только несжатый, PCM), а также MP3, CDA, WMA, APE и FLAC. DeepSound умеет внедрять файлы любого типа и

автоматически рассчитывает доступное для них место в зависимости от размера контейнера и настроек качества аудио.

Программное обеспечение DeepSound не используется для шифрования данных. Скорее, он используется для обнаружения скрытых сообщений, внедренных в аудиосигналы с помощью стеганографических методов.

DeepSound эффективен для обнаружения скрытых сообщений, поскольку он использует глубокие нейронные сети для извлечения сложных особенностей из аудиосигналов. Это позволяет ему идентифицировать даже очень маленькие и хорошо скрытые сообщения.

DeepSound используется для обнаружения скрытых сообщений, внедренных в аудиосигналы с помощью стеганографических методов. Он используется в различных областях, в том числе:

Правоохранительные органы: для обнаружения скрытых сообщений в аудиозаписях, полученных в ходе расследований.

Разведка: для анализа аудиокоммуникаций и обнаружения скрытых сообщений, которые могут содержать секретную информацию.

Кибербезопасность: для выявления и предотвращения вредоносных действий, таких как передача вредоносного ПО или кража конфиденциальной информации.

Исследования: для изучения стеганографических методов и разработки новых методов обнаружения скрытых сообщений.

DeepSound не подходит для скрытия информации по следующим причинам:

1. Обнаружение: DeepSound может с высокой степенью точности обнаруживать скрытые сообщения, что делает его неподходящим для надежного скрытия информации.

2. Потеря данных: Стеганографические методы, обнаруживаемые DeepSound, часто вызывают потерю данных в исходном аудиосигнале, что может снизить его качество.

3. Несовместимость: DeepSound может обнаруживать скрытые сообщения, внедренные только с помощью определенных стеганографических алгоритмов. Это

ограничивает его полезность для скрытия информации, поскольку злоумышленники могут использовать другие алгоритмы, которые не обнаруживаются DeepSound.

Практическая часть

Программа может просто поместить любой файл внутри музыкального, или предварительно зашифровать его по алгоритму AES с длиной ключа 256 бит. Опытным путем было установлено, что предельная длина пароля – всего 32 символа.

Основное отличие между вложением без шифрования и вложением с шифрованием заключается в использовании шифрования для защиты скрытого сообщения. Шифрование добавляет дополнительный уровень безопасности, делая невозможным извлечение скрытого сообщения без ключа шифрования.

Вложение с шифрованием обеспечивает более высокий уровень безопасности, чем вложение без шифрования, поскольку оно защищает скрытое сообщение от извлечения без ключа шифрования. Однако вложение с шифрованием также более сложно реализовать и может замедлить процесс вложения. Выбор между вложением без шифрования и вложением с шифрованием зависит от требуемого уровня безопасности и других факторов, таких как сложность и скорость.

В один контейнер можно поместить любое количество файлов, пока не заполнится счетчик свободного места. Его количество зависит от степени качества (то есть вносимых в аудиофайл искажений). Всего доступны три настройки: высокое, обычное и низкое качество. Каждая из них увеличивает полезный объем контейнера вдвое.

Извлекается стегосообщение после выбора соответствующего контейнера вручную. Если использовалось шифрование, то без ввода пароля программа не покажет даже название скрытого файла. Кириллические символы в названиях файлов не поддерживаются. При извлечении они заменяются на XXXX, однако на содержимое файла это никак не влияет.

DeepSound умеет конвертировать MP3 и CDA, поэтому мы легко можем преобразовать исходный файл из MP3 в WAV и сравнить два контейнера: пустой и заполненный.

Извлекается стегосообщение после выбора соответствующего контейнера вручную. Если использовалось шифрование, то без ввода пароля программа не покажет даже название скрытого файла. Кириллические символы в названиях файлов не поддерживаются. При извлечении они заменяются на XXXX, однако на содержимое файла это никак не влияет.

DeepSound умеет конвертировать MP3 и CDA, поэтому мы легко можем преобразовать исходный файл из MP3 в WAV и сравнить два контейнера: пустой и заполненный.

Объем вложенного сообщения можно оценить в процентах от исходного размера аудиофайла. Например, если исходный аудиофайл размером 1 МБ и скрытое сообщение объемом 100 КБ внедрено с глубиной вложения 50%, то это означает, что скрытое сообщение составляет 10% от размера исходного аудиофайла.

Глубина вложения также влияет на величину искажений звукового файла. Более глубокое вложение приводит к меньшим искажениям, поскольку скрытое сообщение внедряется с меньшей интенсивностью. Величину искажений звукового файла можно оценить с помощью различных метрик, таких как отношение сигнал/шум (SNR) и коэффициент гармонических искажений (THD). Более высокое отношение сигнал/шум и более низкий коэффициент гармонических искажений указывают на меньшие искажения. Для оценки величины искажений при различной глубины вложения можно сравнить значения SNR и THD для аудиофайлов, в которые внедрено скрытое сообщение с различной глубиной.

Глубина вложения является важным параметром, который влияет на объем вложенного сообщения и величину искажений звукового файла. Оценка настроек глубины вложения позволяет оптимизировать процесс вложения для достижения желаемого компромисса между объемом вложенного сообщения, безопасностью и качеством звука

Преобразование формата аудиофайла может повлиять на сохранность вложения. Некоторые форматы аудиофайлов, такие как WAV и AIFF, являются несжатыми и не вносят искажений в аудиосигнал. Другие форматы, такие как MP3 и AAC, используют сжатие с потерями, что может привести к потере данных, включая скрытые сообщения. Для оценки сохранения вложения при преобразованиях формата можно сравнить отношения сигнал/шум (SNR) и коэффициенты гармонических искажений (THD) исходного и преобразованного аудиофайлов. Более низкие значения SNR и более высокие значения THD указывают на большую потерю данных.

Для оценки сохранения вложения при сжатии качества можно сравнить значения SNR и THD исходного и сжатого аудиофайлов. Более низкие значения SNR и более высокие значения THD указывают на большую потерю данных. Другие преобразования, такие как фильтрация, эквализация и нормализация, также могут влиять на сохранность вложения. Эти преобразования могут изменить характеристики аудиосигнала, что может сделать скрытое сообщение более или менее заметным. Для оценки сохранения вложения при других преобразованиях можно сравнить значения SNR и THD исходного и преобразованного аудиофайлов. Более низкие значения SNR и более высокие значения THD указывают на большую потерю данных.

Сохранение вложения при различных преобразованиях файла зависит от типа преобразования и используемых параметров. Оценка сохранения вложения позволяет оптимизировать процесс вложения для обеспечения сохранности скрытого сообщения при различных преобразованиях.

DeepSound обнаруживает файлы с вложениями, анализируя аудиосигналы и извлекая из них характеристики с помощью глубоких нейронных сетей. Эти характеристики затем используются для классификации аудиофайлов как содержащих или не содержащих скрытые сообщения. Модель глубокого обучения DeepSound обучается на большом наборе как чистых, так и стеганографических аудиофайлов. Во время обучения модель учится различать нормальные аудиосигналы и сигналы, содержащие скрытые сообщения. После обучения модель может использоваться

для анализа аудиофайлов и выявления тех, которые, вероятно, содержат скрытые сообщения. DeepSound предоставляет оценку вероятности того, что аудиофайл содержит скрытое сообщение, что позволяет пользователям принимать обоснованные решения о дальнейшем анализе или действиях.

DeepSound- это инструмент, который использует глубокое обучение для обнаружения скрытых сообщений в аудиосигналах. Он имеет следующие возможности:

1. Высокая точность обнаружения даже очень маленьких и хорошо скрытых сообщений

2. Возможность обнаруживать сообщения, внедренные с помощью различных стеганографических алгоритмов

3. Удобный веб-интерфейс и пакет Python для интеграции в пользовательские приложения

DeepSound- это полезный инструмент для обнаружения скрытых сообщений в аудиосигналах, но он не подходит для шифрования информации. Для шифрования информации следует использовать традиционные криптографические алгоритмы.

Оценка устойчивости к атакам DeepSound предоставляет ценную информацию о надежности скрытого сообщения. Более устойчивые сообщения имеют меньшую вероятность быть обнаруженными и удаленными при попытке дестеганографирования. Однако следует отметить, что ни один стеганографический метод не является абсолютно надежным, и устойчивость сообщения всегда является компромиссом между скрытностью и надежностью.

Скрытность, предоставляемая DeepSound, является относительной мерой и может варьироваться в зависимости от используемого стеганографического алгоритма и характеристик аудио. Однако это полезный инструмент для оценки обнаружения скрытых сообщений в аудиосигналах.

Скрытность вложения, обнаруженного DeepSound, зависит от нескольких факторов, включая: тип и сложность используемого стеганографического алгоритма, длина и характер скрытого сообщения и качество и характеристики исходного аудиосигнала

Список литературы:

1. Официальный сайт Deepsound [Электронный ресурс]. URL: https://deepsound.ru.uptodown.com/windows (дата обращения 03.07.2024)
2. Красов, А.В. Методика выявления в доверенной зоне потенциального использования программного обеспечения по созданию нетрадиционных (стеганографических) каналов / А.В. Красов // Наука и бизнес: пути развития. – 2022. – № 4(130). – С. 65-78. – EDN YJNYVO.
3. Коржик, В.И. Цифровая стеганография : учебник / В.И. Коржик, А.В. Красов. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2023. – 324 с. – ISBN 978-5-406-10970-0. – EDN KNKBXU.
4. Шелухин О.И. Цифровая стеганография Технические аспекты управления с использованием сети Интернет : Монография / А.А. Алейников, К.З. Билятдинов, А.В. Красов [и др.]. – Санкт-Петербург : Центр научно-информационных технологий "Астерион", 2016. – 305 с. – ISBN 978-5-00045-408-4. – EDN XGTJLL.
5. Красов, А.В. Модель нарушителя информационной безопасности, использующего стеганографические каналы взаимодействия / А.В. Красов // Наука и бизнес: пути развития. – 2022. – № 4(130). – С. 79-88. – EDN TZAHFJ.
6. Красов, А.В. Модель нарушителя информационной безопасности, использующего методы стеганогрфаии / А.В. Красов // Региональная информатика и информационная безопасность : Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции, Санкт-Петербург, 26–28 октября 2022 года. Том Выпуск 11. – Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2022. – С. 589-592. – EDN RVMFWQ.
7. Цифровая стеганография и цифровые водяные знаки / В.И. Коржик, К.А. Небаева, Е.Ю. Герлинг [и др.] ; Под общей редакцией профессора В.И. Коржика. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – 226 с. – ISBN 978-5-89160-125-3. – EDN WJYYGJ.

ИСПОЛЬЗОВАНИЕ QUICKSTEGO ДЛЯ РЕАЛИЗАЦИИ СКРЫТЫХ СТЕНОГРАФИЧЕСКИХ КАНАЛОВ ВЗАИМОДЕЙСТВИЯ НА ОСНОВЕ МЕТОДА НЗБ

Кузьмин Григорий Алексеевич
студент,
Санкт-Петербургский государственный
университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
РФ, г. Санкт-Петербург

Ченцов Илья Дмитриевич
студент,
Санкт-Петербургский государственный
университет телекоммуникаций
им. проф. М.А. Бонч-Бруевича,
РФ, г. Санкт-Петербург

USE OF QUICKSTEGO TO REALIZE HIDDEN STENOGRAPHIC LSB-BASED COMMUNICATION CHANNELS

Grigoriy Kuzmin
Student,
Prof.M. A. Bonch-Bruevich St. Petersburg State University
of Telecommunications
Bolshevikov Ave,
Russia, Saint-Petersburg

Ilya Chentsov
Student,
Prof.M. A. Bonch-Bruevich St. Petersburg State University
of Telecommunications
Bolshevikov Ave,
Russia, Saint-Petersburg

Аннотация. Данная работа исследует применение программного инструмента QuickStego для создания скрытых стеганографических каналов на основе наименьших значащих бит (НЗБ). QuickStego представляет собой удобное приложение для скрытия информации в изображениях с использованием различных методов стеганографии. Будут проанализированы технические аспекты использования QuickStego для реализации скрытых стеганографических каналов, а также

рассмотрены возможности обнаружения и защиты от подобных методов передачи информации.

Abstract. This paper investigates the application of QuickStego software tool to create hidden steganographic channels based on least significant bits (LSB). QuickStego is a user-friendly application for hiding information in images using various steganography techniques. The technical aspects of using QuickStego to implement hidden steganographic channels will be analyzed, and the possibilities of detection and protection against such methods of information transfer will be considered.

Ключевые слова: Стеганография, стеганографические методы, сокрытие информации, метод наименьших значащих бит, НЗБ, QuickStego

Keywords: Steganography, steganographic methods, information hiding, least significant bit method, LSB, QuickStego

Введение. Образовательная система в информационном обществе должна стать системой опережающей. Переход от консервативной образовательной системы к опережающей должен базироваться на опережающем формировании информационного пространства Российского образования.

Введение

Стеганография, искусство сокрытия информации в неприметных носителях, имеет первостепенное значение в современном цифровом мире. Оно позволяет скрывать чувствительные данные, такие как личная информация, финансовые данные и коммерческие секреты, в обычных файлах изображений, аудио и видеофайлах, обеспечивая дополнительный уровень безопасности для конфиденциальных коммуникаций, предотвращая несанкционированный доступ к данным. Так же, стеганография может применяться для незаметного внедрения меток авторских прав или водяных знаков в цифровые медиафайлы, помогая защитить интеллектуальную собственность и отслеживать несанкционированное использование контента.

Цель:

Изучить и понять алгоритм и принципы работы стеганографического инструмента QuickStego для реализации скрытых каналов взаимодействия на основе метода НЗБ (наименьших значащих битов).

Разработать программное обеспечение или расширение для реализации стеганографических каналов взаимодействия с использованием QuickStego и метода НЗБ.

Оценить эффективность и надежность разработанных стеганографических каналов взаимодействия.

Задачи:

- Изучить алгоритм метода НЗБ и его применение в стеганографии.
- Провести тестирование и оценку стеганографических каналов взаимодействия с использованием различных типов файлов-носителей и различных параметров встраивания.
- Определить возможности и ограничения использования стеганографических каналов взаимодействия в реальных условиях.
- Подготовить отчет или публикацию с описанием проведенной работы, полученных результатов и сделанных выводов.

Стеганография – метод передачи или хранения информации с учетом того, что факт такой передачи (хранения) сохраняется в тайне. Таким образом, в отличие от криптографии, стеганография скрывает само существование секретного сообщения. Информация скрыта в объекте-носителе или контейнере, и после добавления сообщения объект-носитель должен выглядеть «обычным», чтобы присутствие в нем скрытого сообщения было незаметно для стороннего наблюдателя. Поскольку стеганография никак не шифрует скрытую информацию, помимо криптографических используются стеганографические методы.

Стеганографию можно использовать для сокрытия информации в различных типах цифровых данных: тексте, изображениях, аудио- и видеофайлах. В этом смысле цифровые изображения представляют собой едва ли не самый популярный

формат медиаобъектов, поскольку они имеют большие размеры и не вызывают подозрений при публикации в социальных сетях и отправке по электронной почте.

Стеганографические методы, то есть методы внедрения секретного сообщения в объект-носитель, обычно оцениваются по нескольким критериям:

- незаметность – в случае цифрового изображения человек не должен видеть разницу между исходным изображением и изображением с заложенным в него секретным посланием;
- емкость встраивания – максимальный объем данных, который можно вставить в объект-носитель;
- надежность – способность сообщения противостоять искажениям, вносимым при обработке или передаче объекта-контейнера, например, при сжатии или редактировании (повороте или перевороте) изображения. Подобные искажения иногда используются для целенаправленного повреждения стеганограммы.

Стеганографические методы обработки цифровых изображений делятся на два класса: пространственные методы (или методы для временной области) и частотные методы (или методы для частотной области). Пространственные методы манипулируют значениями в пространственной области – пикселях. Частотные методы – частотные характеристики изображения.

В этой статье будет рассмотрен метод наименьшего значащего бита (LSB) – это простой и распространенный способ сокрытия информации в цифровых изображениях, который относится к пространственным методам стеганографии. Он работает путем изменения наименее значимых битов каждого пикселя в изображении.

Метод LSB (младшего значащего бита) имеет исторические корни в двоичной математике. Упоминания о нем можно найти в работах известного математика и логика, как Готфрид Вильгельм Лейбниц, в 17 веке. Однако важность битовых манипуляций для передачи и хранения данных была подчеркнута в статье Клода Шеннона "Математическая теория связи" в 1948 году.

В 1991 году Шамир Адлеман и Брослав Маркелл предложили использовать метод LSB для скрытого встраивания сообщений в изображения. Их исследование было связано с разработкой цифрового водяного знака, который представляет собой способ защиты цифровых данных и авторских прав путем невидимого встраивания маркеров в изображения.

Алгоритм:

1. Секретные данные (например, текст) преобразуются в последовательность битов (двоичный формат).

2. Извлечение пикселей: Цифровое изображение представляется как сетка пикселей, каждый из которых имеет три цветовых компонента: красный, зеленый и синий (Red, Green, Blue – RGB).

3. Наименее значимый бит каждого цветового компонента пикселя заменяется соответствующим битом секретных данных.

4. Измененный набор пикселей сохраняется как новое изображение.

Цифровые графические изображения получаются из аналоговой формы путем двоичного кодирования информации и представляют собой матрицу пикселей. Пиксель – это единичный элемент изображения с фиксированными координатами и одним четко определенным цветом. Поэтому, для определения информационного объема графического изображения требуется знать разрешающую способность экрана и глубину цвета пикселя. Каждый цвет можно рассматривать как возможное состояние точки, тогда количество цветов, отображаемых на экране монитора, может быть вычислено по формуле:

$$\boldsymbol{N = 2^i} \qquad \textbf{(1)}$$

где i – глубина цвета кода

Необходимый объем видеопамяти рассчитывается так: количество всех точек на экране умножается на глубину цвета одной точки. Например, чтобы определить глубину цвета в графическом режиме True Color, в котором палитра

состоит более чем из 4-х миллиардов цветов (N = 4 294 967 296 цветов), используем формулу:

$$log_2(4294967296) = 32 \quad (2)$$

Допустим, имеется простое 8-битное изображение в градациях серого. В этом случае 00h (00000000b) обозначает черный цвет пикселя, FFh (11111111b) – белый, все остальное – градации серого. Всего имеется 256 градаций (2 в степени 8). Также предположим, что сообщение (файл) состоит из 1 байта – например, 01101011b. Если изменить любой байт такого файла или (что одно и то же) отдельные биты этого байта, то соответствующий ему пиксель изменит яркость. При этом изменение разных битов влияет на яркость пикселя по-разному: первый очень сильно, второй слабее, а последний, восьмой бит может добавить байту (а значит, и пикселю) только единицу. При использовании 2 младших бит в описаниях пикселей, нам потребуется 4 пикселя. Допустим, они черного цвета. Тогда пиксели, содержащие скрытое сообщение, будут выглядеть следующим образом: 00000001 00000010 00000010 00000011. Тогда цвет пикселей изменится: первого – на 1/255, второго и третьего – на 2/255 и четвертого – на 3/255.

Нормальный человек не заметит изменение яркости точки на 1/255 градацию серого. А значит, абсолютно не важно, каковы последние биты каждого байта. И их можно обнулять, переставлять, заменять; картинка при этом будет казаться одинаковой.

Автором утилиты OpenStego указан Самир Вайдья (Samir Vaidya) - профессор математики из университета Саураштра города Раджкот штата Гуджарат, Индия.

Последнее выпущенное обновление OpenStego (версия 0.61) датируется 2014 годом. Эта программа совместима с операционными системами Windows и Linux. Она способна обрабатывать изображения в форматах BMP, PNG, JPG, GIF и WBMP, а также всегда сохраняет заполненный контейнер в формате PNG. Кроме того, размер OpenStego составляет всего 203 Кбайт. Так же, OpenStego имеет открытый код и использует метод НЗБ (LSB).

Для сокрытия данных я взял фото формата PNG, как стегоконтейнер и другое фото того же формата, как данные. Вносим пути этих файлов в строки «Message file» (Файл с сообщением) и «Cover file» (Файл обложки). Далее выбираем имя нашего нового файла в строке «Output stego file» (Выходной стего-файл) и нажимаем кнопку «Hide data» (Скрыть данные) (Рис 1).

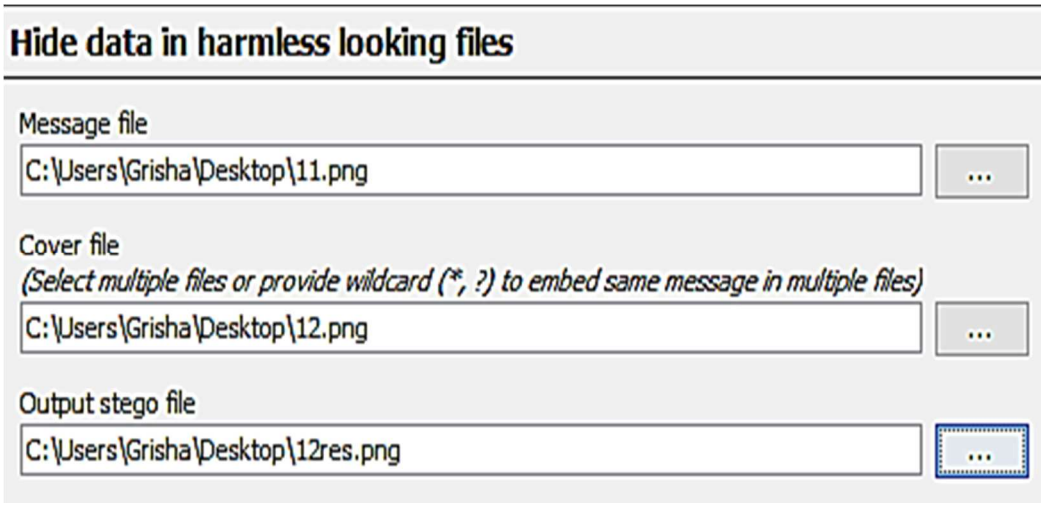


Рисунок 1. Пример

Получилась картинка, внешне неотличимая от изначальной (Рис 2 и Рис 3)

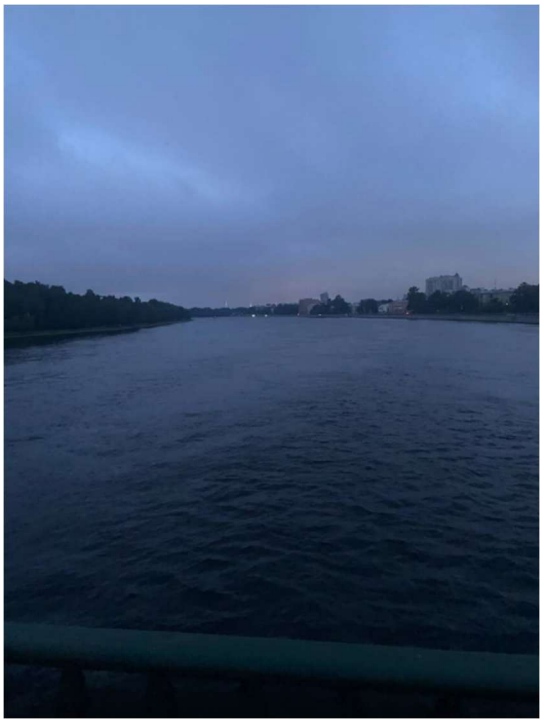


Рисунок 2. Изначальное фото (12.png)

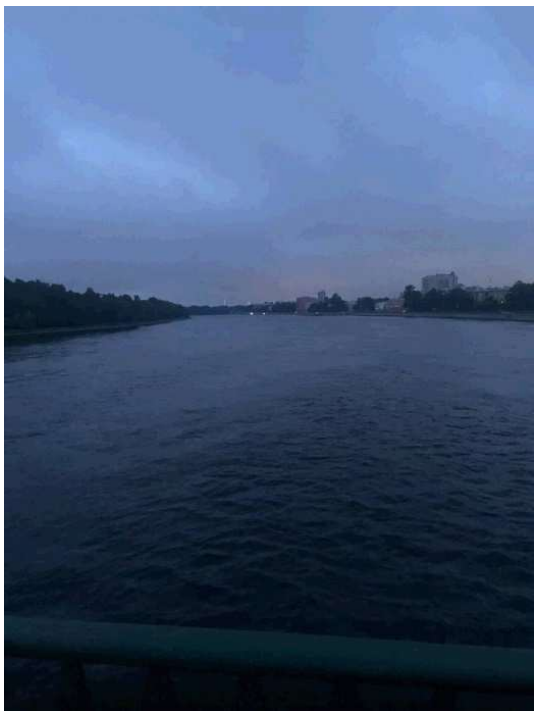


Рисунок 3. Фото со скрытыми данными (12res.png)

Но если сравнить размеры файла, то они отличаются (Рис 4 и Рис 5)

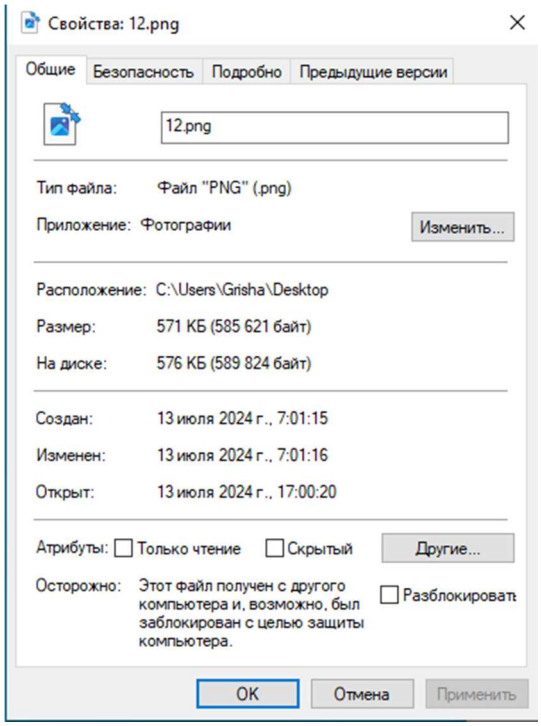


Рисунок 4. Размер изначального изображения

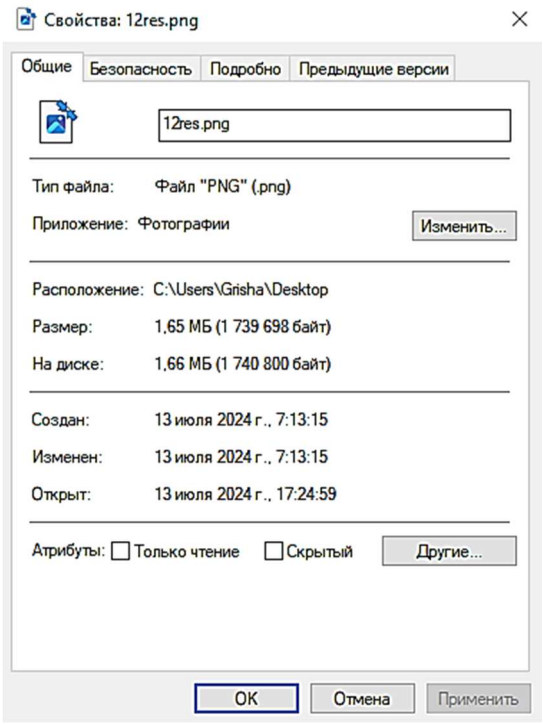


Рисунок 5. Размер конечного изображения

Так же, при побайтном сравнении с оригиналом отличия будут во всех значениях сразу после заголовка (Рис 6 и Рис 7).

Рисунок 6. байты исходного файла

Рисунок 7. байты конечного файла

При архивировании и последующем разархивировании конечного файла данные так же можно извлечь, но если поменять формат файла (например, на JPG) то утилита выдаст ошибку, даже если потом перевести изображение в формат PNG (Рис 8).

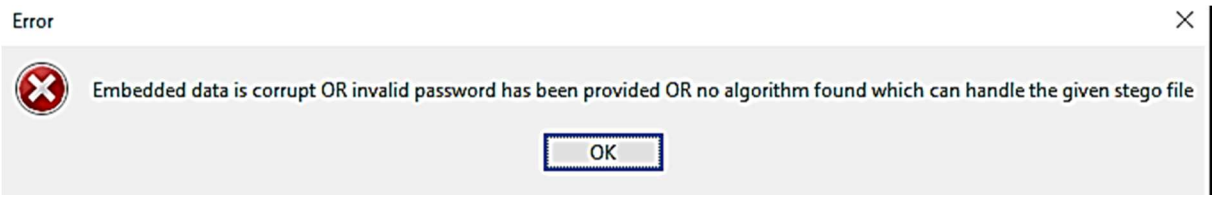


Рисунок 1. Ошибка

Рисунок 9. Перевод ошибки

В исследовании была проведена всесторонняя оценка утилиты OpenStego для стеганографии с использованием метода НЗБ (LSB). Программа неплохо

показала себя в кодировании изображений. Сама утилиты испытывает проблемы при работе с файлом после изменения формата, но справляется с файлом, после архивации. А метод НЗБ (LSB) предоставил показательные результаты в скорости работы и своём функционале. Невооруженным глазом исходное и конечное изображение не отличить, но при более подробном изучении есть отличия. Лучше всего использовать метод НЗБ (LSB) там, где искать информацию будут с наименьшей вероятность, потому что метод не отличается высокой степенью сложности.

Список литературы:

1. Коржик, В.И. Цифровая стеганография : учебник / В.И. Коржик, А.В. Красов. – Москва : Общество с ограниченной ответственностью "Издательство "КноРус", 2023. – 324 с. – ISBN 978-5-406-10970-0. – EDN KNKBXU.
2. Красов, А.В. Модель нарушителя информационной безопасности, использующего методы стеганогрфаии / А.В. Красов // Региональная информатика и информационная безопасность : Сборник трудов Юбилейной XVIII Санкт-Петербургской международной конференции, Санкт-Петербург, 26–28 октября 2022 года. Том Выпуск 11. – Санкт-Петербург: Региональная общественная организация "Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления", 2022. – С. 589-592. – EDN RVMFWQ.
3. OpenStego [Электронный ресурс]. URL: https://www.openstego.com (дата обращения 08.07.2024)
4. Коржик В.И., Нгуен З.К., Даньшина А.В. Обнаружение стегосистем, использующих погружение конфиденциальной информации в контуры изображения. Том 13 – Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, Россия: научная статья, 2021, 75-85 с, ISSN: 2409-5419
5. Цифровая стеганография и цифровые водяные знаки / В.И. Коржик, К.А. Небаева, Е.Ю. Герлинг [и др.] ; Под общей редакцией профессора В.И. Коржика. Том Часть 1. – Санкт-Петербург : Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2016. – 226 с. – ISBN 978-5-89160-125-3. – EDN WJYYGJ.
6. Бабаш А.В. Криптографические методы защиты информации: учебник для вузов / А.В. Бабаш, Е.К. Баранова - Москва: КноРус, 2016 - 189 с. - ISBN 978-5-406-04766-8.
7. 21 лучший инструмент для обеспечения безопасности ваших данных [Электронный ресурс]. URL: https://technicalustad.com/steganography-tools/ (дата обращения 12.07.2024).

ДЛЯ ЗАМЕТОК

МОЛОДЕЖНЫЙ НАУЧНЫЙ ФОРУМ:

Электронный сборник статей по материалам CCLVIII студенческой международной научно-практической конференции

№ 26 (258)
Июль 2024 г.

В авторской редакции

Издательство «МЦНО»
123098, г. Москва, ул. Маршала Василевского, дом 5, корпус 1, к. 74
E-mail: mail@nauchforum.ru

16+