**Стеганография текста**

***Варнавский М.А. Ионисян А С.***

*Государственное автономное образовательное учреждение дополнительного образования «Центр для одаренных детей „Поиск“»*

*г. Ставрополь, Россия,*

*Email:* [*matvei.varnavskii@gmail.com*](mailto:matvei.varnavskii@gmail.com)*, asion@mail.ru*

**Text steganography**

***Varnavsky M.A. Ionisyan A. S.***

*State Autonomous Educational Institution of Additional Education "Poisk Center for Gifted Children"*

*Stavropol, Russia*

**Аннотация**

изучен стенографический метод сокрытия текста в цифровом изображении и создана компьютерная программа на языке программирования Python, обладающая графическим пользовательским интерфейсом, для ввода текстовой информации и её сокрытия, извлечения и вывода информации в графическом файле формата BMP.

**Abstract**

A steganographic method of hiding text in a digital image has been studied and a computer program has been created in the Python programming language with a graphical user interface for entering text information and hiding it, extracting and outputting information in a graphical BMP file.

**Ключевые слова:** обработка текстовой информации; обработка графической информации; стеганография.

**Keywords:** text information processing; graphic information processing; steganography.

**Введение.**

Стеганография – это метод скрытой передачи информации, при котором данные внедряются в другой носитель таким образом, чтобы их наличие было незаметно для стороннего наблюдателя. В случае цифровой графики, текст может быть спрятан внутри изображений без видимых изменений самого изображения. Этот процесс осуществляется путем изменения отдельных битов пикселей, так что человеческому глазу такие модификации остаются незаметными.

Целевой аудиторией программы являются те люди, которые беспокоятся о безопасности своих данных при хранении на компьютере или при пересылке через Интернет.

Проект является актуальным, так как повышает безопасность хранения важной информации на персональном компьютере и ее пересылку в сокрытом от посторонних глаз виде.

**Анализ существующих решений и методов.**

Существует большое количество готовых программ для стеганографии:

1. Steghide - это одна из самых известных утилит командной строки для стеганографии. Она позволяет встраивать текстовые сообщения или файлы в изображения и аудиофайлы. Программа обеспечивает поддержку различных форматов изображений (BMP, JPEG) и аудио форматов (WAV), может использовать пароль для дополнительной защиты скрытого содержимого.
2. OpenPuff – это мощная программа для стеганографии, поддерживающая множество типов контейнеров, включая изображения, звуковые файлы, видеофайлы и даже двоичные 3 файлы. Она поддерживает шифрование встроенных данных с использованием алгоритмов AES, Blowfish и других. Имеет графический пользовательский интерфейс, что упрощает ее использование.
3. OutGuess – это инструмент командной строки, предназначенный для встраивания данных в изображения формата JPEG. Особенностью данной программы является высокий уровень устойчивости к обнаружению благодаря использованию метода замены наименее значимых битов. Программа работает с изображениями без видимых изменений качества.
4. Snow – это простой инструмент командной строки для встраивания текста в обычные текстовые файлы. Метод работы основан на использовании пробелов между словами для передачи скрытой информации. Подходит для случаев, когда необходимо скрыть небольшие объемы данных.
5. QuickStego – это простая программа для Windows, предназначенная для быстрой и легкой интеграции данных в изображения. Имеет очень простой интерфейс, подходящий для новичков, возможность выбора уровня сжатия JPEG для сохранения качества изображения.

Эти программы охватывают различные аспекты стеганографии, начиная от простых инструментов для быстрого внедрения данных до сложных систем с поддержкой множества методов и форматов.

В данном проекте используется простейший, но оригинальный алгоритм сокрытия текста в цифровом графическом изображении, что делает программу очень быстрой и позволяет скрывать в одном цифровом изображении сразу несколько разных текстовых сообщений. Интерфейс программы основан на использовании библиотеки Qt5, поэтому пользоваться программой удобно.

**Ресурсное обеспечение проекта.**

Проект состоит из исходного кода на языке python — файл pyStegano.py и описания графического пользовательского интерфейса — файла puSteganoUI.py. Графический интерфейс создавался в программе QtDesigner и был сохранен в файле pySteganoUI.ui.

Далее этот файл при помощи утилиты pyuic преобразовывался в pySteganoUI.py. Так как программа была написана с использованием функций модуля pyQt5, то для запуска программы потребуется, чтобы pyQt5 и библиотека Qt5 были заранее установлены на компьютере пользователя. Библиотека pyQt5 хорошо работает с python версий от 3.7 до 3.10. Для других версий python возможны так называемые «глюки» и отказы в запуске программы.

Для того, чтобы можно было скрывать текст в графическом файле нужно иметь несколько графических файлов любого размера в популярных форматах BMP, JPG, PNG и т. п., в которых и будет спрятана текстовая информация. Если таких файлов нет, то программа pyStegano сама создаст графический файл формата BMP размером 256х256 пикселей черного цвета. Некоторые из этих пикселей будут немного светлее остальных после помещения в них текста, что незаметно на глаз, но может быть выявлено, если усилить контрастность изображения.

**Полученный результат**

Мной была создана компьютерная программа pyStegano, которая позволяет скрывать текстовую информацию в цифровом графическом файле формата BMP. Полный исходный текст этой программы на языке программирования Python приведен в приложении. Для запуска программы нужно перейти в рабочий каталог программы, запустить терминал и ввести в нем команду python pyStegano.py. На рисунке 1 показан внешний вид программы сразу после запуска.

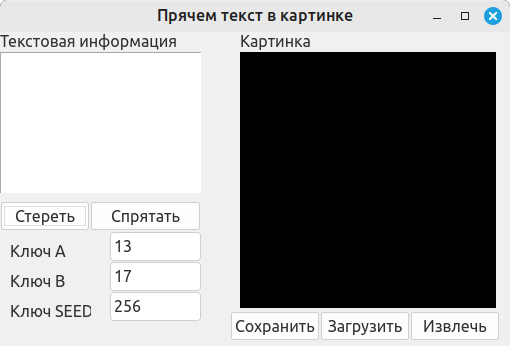


Рисунок 1. - Программа pyStegano после запуска

В главном окне pyStegano содержится:

1. Поле для ввода текстовой информации, которую нужно скрыть.
2. Кнопка «Стереть», которая стирает введенную в поле ввода текстовую информацию, (из картинки информация не стирается).
3. Кнопка «Спрятать», нажав на которую запустится процесс скрытия информации из поля ввода в картинку.
4. Поля ввода «Ключ A», «Ключ B» и «Ключ SEED», которые позволяют настроить параметры шифрования и скрывать в одной картинке сразу несколько текстовых сообщений одновременно.
5. Метка «Картинка», в которой отображается загруженный цифровой графический файл до и после сокрытия в нем текстовой информации.
6. Кнопка «Загрузить», предназначенная для выбора картинки, в которую нужно спрятать текстовое сообщение или из которой нужно извлечь текстовое сообщение.
7. Кнопка «Сохранить», предназначенная для выбора имени файла, в который нужно сохранить картинку с сокрытой в ней текстовой информацией.
8. Кнопка «Извлечь», нажав на которую запустится процесс извлечения текстовой информации из загруженной картинки.

Сразу после запуска программы будет сформировано чистое черное изображение размером 256 на 256 пикселей, пригодное для сокрытия в нем текстовых сообщений.

Алгоритм работы с программой состоит в выполнении следующих шагов:

1. Ввести или скопировать в поле ввода текста текст, который нужно спрятать.
2. Проверить ключи шифрования. Ключ А должен давать 1 в остатке от деления на 4, а ключ B быть нечетным числом. Ключ SEED — это число от 1 до 65535 - номер пикселя в картинке, начиная от которого и будет спрятан текст. Выбирая разные значения A, B и SEED в одной картинке можно прятать сразу несколько небольших текстовых сообщений.
3. Нажав на кнопку «Загрузить», выбрать и загрузить картинку, в которую будет спрятан текст.
4. Нажать на кнопку «Скрыть».
5. Нажать кнопку «Сохранить» для сохранения полученной картинки с закодированным в ней текстом (см. рисунок)

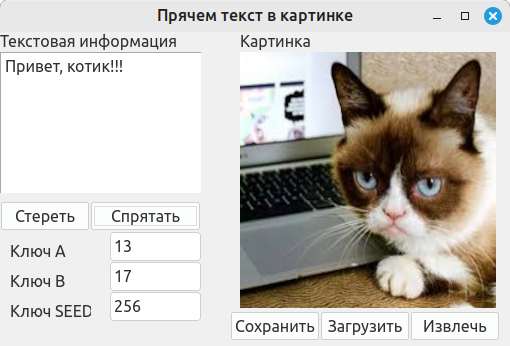


Рисунок 2. - Внешний вид программы после выполнения шагов алгоритма сокрытия текста в картинке

Чтобы извлечь текстовую информацию из картинки, в которую ранее был спрятан текст, нужно загрузить эту картинку кнопкой «Загрузить», проверить параметры шифрования (ключи A, B и SEED) и нажать кнопку «Извлечь». Если в картинке был спрятан текст, то он отобразится в окне текстовой информации (см. рисунок)

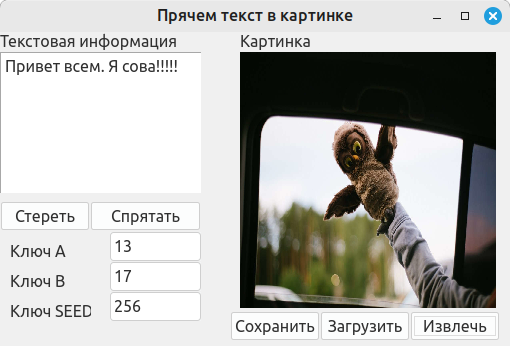


Рисунок 3. - Из картинки совы извлечено текстовое сообщение «Привет всем. Я сова!!!!»

Математический алгоритм работы программы состоит в генерации последовательности псевдослучайных чисел от 0 до 65535, каждое из которых — это номер пикселя, который нужно слегка модифицировать, а именно заменить два младших бита на очередные биты символов текстового сообщения. Перед текстовым сообщением в картинку прячется 16- битовое число — размер текстового сообщения в символах. Программа работает с текстом в формате UTF8, в котором каждый символ кодируется 16 битами и сохранения каждого символа модифицирует 4 пикселя.

Для расчета псевдослучайной последовательности используется формула:

pos\_next=(A\*pos\_cur+B) mod 65536

где pos\_next — псевдослучайный номер следующего пикселя,

pos\_cur — номер текущего пикселя (первый модифицируемый пиксель имеет номер SEED),

A и B — ключи шифрования (A mod 4 =1, B — нечетное),

mod — операция расчета остатка от деления.

Проведенные эксперименты показали, что в картинке размером 256х256 пикселей можно спрятать текстовое сообщение размером до 16380 символов так, что внешне картинка до модификации и после модификации не отличаются.

**Используемые источники**

1. Описание методов стеганографии в открытой интернет-библиотеке «Википедия». // https://ru.wikipedia.org/wiki/Стеганография

2. Среда программирования Pycharm. // <https://www.jetbrains.com/pycharm/>

3. Язык программирования Python. // <https://www.python.org/>

4. Библиотека создания графического интерфейса Qt5. // <https://www.qt.io/>

6. Учебный проект «Стеганография текста» // [электронный ресурс] https://github.com/anserion/pyStegano