УДК 004.056.55

СТЕГАНОГРАФИЧЕСКИЙ МЕТОД ЗАЩИТЫ ИНФОРМАЦИИ

Д.С. Серкевич, Ю.О. Герман
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В данной статье рассмотрены методы защиты информации с использованием стеганографии, а также предложен вариант для стеганографического скрытия текстовой информации, реализующий метод обратимого сокрытия текстовой информации в изображениях формата JPEG с использованием техники замены наименьшего значащего бита. Представлена актуальность развития методов стеганографии в сфере кибербезопасности.
Ключевые слова: стеганография; LSB; JPEG; цифровые изображения; DCT; RGB; энтропийное кодирование.

STEGANOGRAPHIC METHOD OF INFORMATION PROTECTION

D.S. Serkevich, Yu.O. German
Belarusian State University of Informatics and Radioelectronics Minsk, Republic of Belarus

Abstract. This article examines methods of protecting information using steganography and proposes a method for steganographic concealment of text information, implementing a method for reversibly concealing text information in JPEG images using the least significant bit substitution technique. The relevance of developing steganographic methods in the field of cybersecurity is presented.

Keywords: steganography; LSB; JPEG; digital images; DCT; RGB; entropy coding.

Введение

Стеганография – это метод организации связи (передачи сообщений), при котором скрывается само наличие связи. Основная цель стеганографии – скрыть сам факт передачи сообщения, в отличие от криптографии, которая шифрует содержание, но не скрывает саму передачу. Цифровые изображения являются одними из наиболее распространенных контейнеров для стеганографического встраивания информации благодаря их широкому распространению и избыточности данных. Формат JPEG, будучи наиболее популярным форматом для хранения и передачи фотографических изображений, представляет особый интерес для исследователей и разработчиков стеганографических систем.

Основная часть

Метод LSB является одним из наиболее простых и распространенных алгоритмов стеганографии. Он основан на замене младших битов в битовом представлении значений цветовых компонент пикселей изображения битами скрываемого сообщения.

Каждый пиксель цифрового изображения в цветовой модели RGB представлен тремя байтами, соответствующими интенсивности красного, зеленого и синего каналов. Изменение наименьшего значащего бита каждого канала приводит к изменению яркости цвета, что для человеческого глаза остается практически незаметным. Вклад наименее значимого бита в цвет пикселя незначителен, однако при реверсировании порядка битов в байте его роль становится важной.

Формат JPEG использует сжатие с потерями, основанное на дискретном косинусном преобразовании (DCT).

Процесс сжатия включает следующие этапы: преобразование цветового пространства RGB в YCbCr; разбиение изображения на блоки 8×8 пикселей; применение дискретного косинусного преобразования к каждому блоку; квантование DCT-коэффициентов; энтропийное кодирование.

Важной особенностью *JPEG* является то, что при повторном сохранении изображения происходит повторное квантование *DCT*-коэффициентов, что может разрушить встроенную информацию. Поэтому стеганографические системы для *JPEG* должны либо работать с *DCT*-коэффициентами до этапа квантования, либо учитывать особенности повторного сжатия.

Разработанное программное обеспечение имеет модульную архитектуру, включающую следующие компоненты:

1) модуль работы с изображениями – отвечает за загрузку, обработку и сохранение изображений с сохранением метаданных;

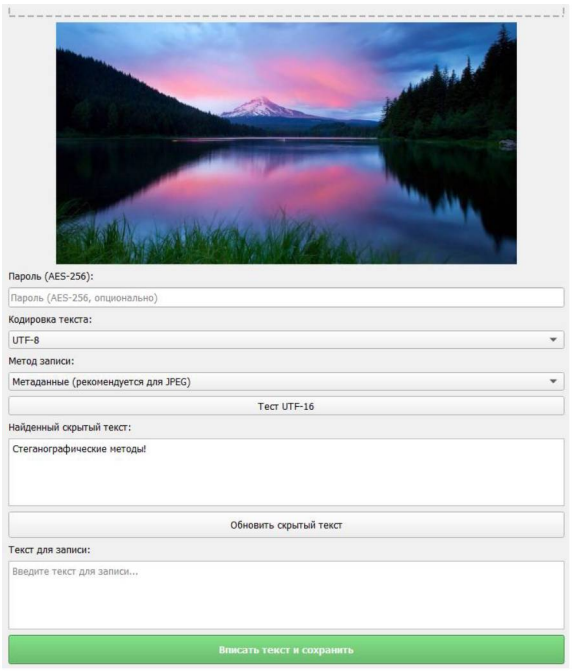
2) модуль кодирования – реализует алгоритмы встраивания текста в *LSB* пикселей;

3) модуль декодирования – извлекает скрытую информацию из изображения;

4) модуль шифрования – обеспечивает дополнительную защиту сообщения с использованием симметричного шифрования;

5) графический интерфейс – предоставляет удобные средства взаимодействия с пользователем (рисунок).

Такая архитектура обеспечивает гибкость, возможность независимого тестирования компонентов и легкость.



Графический интерфейс, разработанного программного обеспечения
Graphical interface of the developed software

Заключение

В данной статье были рассмотрены некоторые из основных методов стеганографии изображений для временной области и преобразования области определения. В процессе создания приложения были изучены теоретические основы стеганографии, проведен сравнительный анализ с криптографией, а также детально рассмотрены особенности представления графических данных в формате JPEG и влияние процесса сжатия с потерями на возможность встраивания конфиденциальных данных.

Реализованная модульная архитектура позволила эффективно разделить функционал по работе с изображениями, кодированию и декодированию сообщений, а также обеспечить дополнительную защиту информации путем ее предварительного шифрования. Разработанный графический интерфейс делает инструмент доступным для пользователя.

Список использованных источников

1. Грибунин В.Г., Оков И.Н., Туринцев И.В. (2009) *Цифровая стеганография. Аспекты защиты.* Москва, Издательство «Солон-Пресс».

2. Окатов А.В. (2016) *Методы цифровой стеганографии.* Санкт-Петербург, Издательство «ГУАП».

References

1. Gribunin V.G., Okov I.N., Turintsev I.V. (2009) *Digital Steganography: Security Aspects*. Moscow, Solon-Press Publishing House (in Russian).

2. Okatov A.V. (2016) *Methods of digital steganography*. St. Petersburg, GUAP Publishing House (in Russian).

Сведения об авторах

Серкевич Д.С., магистрант, кафедра защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», sdasha695@gmail.com.

Герман Ю.О., кандидат технических наук, доцент, доцент кафедры информационных технологий автоматизированных систем, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», jgerman@bsuir.by.

Information about the authors

Serkevich D.S., student, Department of Information Security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", sdasha695@gmail.com.

German Yu.O., Cand. Sci. (Tech.), Associate Professor, Associate Professor of the Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", jgerman@bsuir.by.