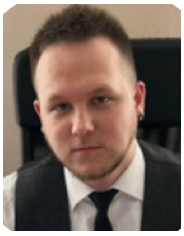
УДК 004.021:004.75

СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ СОКРЫТИЯ ИНФОРМАЦИИ

И.В. Лосик
Студент факультета компьютерных систем и сете по специальности "Вычислительные машины системы и сети"
losikivan2002@gmail.com

С.Н. Нестеренков
Декан факультета компьютерных систем и сетей Белорусского государственного университета информатики и радиоэлектроники, доцент кафедры программного обеспечения информационных технологий
s.nesterenkov@bsuir.by



Д.В. Низовцов
Начальник отдела информационных технологий, ассистент кафедры ПОИТ
d.nizovtzov@bsuir.by

И.В. Лосик
Окончил Минский радиотехнический институт. Область научных интересов связана с разработкой методов и алгоритмов построения информационно-компьютерных систем, организацией учебного и научно-исследовательского процессов в техническом университете.

С.Н. Нестеренков
Кандидат технических наук, доцент, декан факультета компьютерных систем и сетей Белорусского государственного университета информатики и радиоэлектроники, доцент кафедры программного обеспечения информационных технологий. Автор публикаций на тему машинного обучения, алгоритмов принятия решений, искусственных нейронных сетей и автоматизации

Д.В. Низовцов
Окончил БГУИР в 2016 году по специальности "Программное обеспечение информационных технологий", магистрант первого года обучения по специальности "Электронные системы и технологии" БГУИР.

Аннотация. В данной работе были рассмотрены принципы стеганографических методов, различные алгоритмы сокрытия информации и инструменты для их обнаружения. Также была поднята тема актуальности развития методов стеганографии и инструментов для их обнаружения в сфере кибербезопасности. Понимание стеганографических методов и их применение может помочь защитить данные от несанкционированного доступа и сохранить конфиденциальность личной информации.

Ключевые слова: Стеганография, LSB, криптография, кибербезопасность.

Введение.

Стеганография - это технология, которая позволяет скрыто передавать сообщение в другом сообщении таким образом, чтобы даже его наличие оставалось незамеченным. Эта технология может использоваться для защиты конфиденциальной информации при ее передаче через интернет или другие открытые коммуникационные среды. Стеганографические методы сокрытия информации могут быть использованы в различных областях, например, в криминалистике, государственной безопасности, бизнесе. Они

позволяют скрыть конфиденциальную информацию, например, финансовые данные или персональные данные.

Актуальность.

Эта технология становится все более популярной в различных областях, в том числе в области кибербезопасности, обмена личными данными, медицинских записей и т.д. Она также может использоваться для целей, связанных с правоохранительными органами и военными. Из-за своей актуальности и важности стеганографические методы сокрытия информации становятся объектом внимания исследований и разработок в области информационных технологий.

Анализ принципов работы метода LSB.

Одним из примеров стеганографического метода является сокрытие информации в видеороликах или изображениях. Это может быть достигнуто путем изменения пикселей изображения или встраивания информации в частотный спектр аудио- или видеофайла. Другим примером может быть сокрытие информации в текстовых файлах, где каждый символ в файле может использоваться для передачи битов информации.

Далее будет рассмотрен Метод Least Significant Bit.

(LSB) Метод Least Significant Bit (LSB) - это один из самых простых методов стеганографии, который использует наименее значимый бит в каждом байте изображения для сокрытия данных. Этот метод позволяет встраивать данные в любой формат изображения без сильного визуального искажения оригинального изображения. Представим изображение на рисунке1 в виде матрицы (рисунок 2), в которой каждая ячейка выражает пиксель, а её значение – цвет этого пикселя/ячейки.

– *Рисунок 1.* Исходное изображение

$$P_{3,3} = \begin{pmatrix} 10000110 & 00101111 & 00000000 \\ 11111111 & 11111111 & 00000000 \\ 11000001 & 00101111 & 00000000 \end{pmatrix}$$

–*Рисунок 2.* Матрица, составленная на основе изображения

–

–Изменим младший бит. Для этого реверсируем их и посмотрим, как в итоге будут выглядеть матрица и новое фото (рисунок 3).

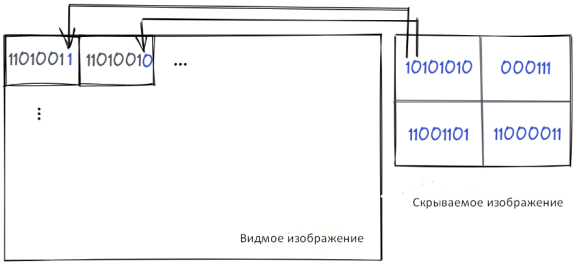
–

$$P_{3,3} = \begin{pmatrix} 10000111 & 00101110 & 00000001 \\ 11111110 & 11111110 & 00000001 \\ 11000000 & 00101110 & 00000001 \end{pmatrix}$$

– *Рисунок 3.* Матрица и изображение, полученные после изменения младших битов исходного изображения

–

–Значительного визуального изменения не произошло, но матрица изображения была изменена и именно на этом и построен метод LSB. На рисунке 4 представлен общий принцип этого метода.



– *Рисунок 4.* Исходное изображение

–

–Существует еще несколько методов стеганографического сокрытия информации, которые могут быть использованы для передачи информации незаметно. Рассмотрим наиболее распространенные из них:

–1. Метод расширения спектра - этот метод используется для сокрытия информации в частотном спектре звукового или видео файла. Для этого используются математические алгоритмы, которые изменяют соотношение между высокими и низкими частотами в звуковой или видеодорожке. Однако этот метод может изменять качество звука или видео, что может привести к потере информации.

–2. Метод сокрытия в фоне - этот метод использует несколько изображений или фрагментов изображений, чтобы сокрыть информацию. Например, можно скрыть сообщение в градиентах цвета или в малозаметном участке изображения. Этот метод является достаточно сложным и менее эффективным, но при правильном использовании может быть достаточно эффективным.

–3. Метод сокрытия в текстовых файлах - этот метод использует изменение символов в текстовых файлах для сокрытия информации. Например, каждый символ может быть использован для передачи одного бита информации. Этот метод является одним из самых простых и эффективных, но может быть детектирован специальными программами, что может привести к раскрытию информации.

–4. Метод сокрытия в сетевом трафике - этот метод используется для передачи информации через сетевой трафик. Например, информация может быть скрыта в интервалах между пакетами или в качестве фонового шума. Этот метод также достаточно сложен и может быть детектирован специальными программами, что может привести к раскрытию информации.

Заключение.

В целом, можно сказать, что стеганографические методы сокрытия информации являются важным инструментом для защиты конфиденциальных данных в различных сферах жизни. Они позволяют закодировать и скрыть информацию внутри другой информации, что делает ее неразличимой при поверхностном рассмотрении. Важно отметить, что развитие стеганографических методов и инструментов для их обнаружения является актуальной темой исследований в области информационных технологий и кибербезопасности. Необходимо прикладывать все усилия для того, чтобы гарантировать безопасность и конфиденциальность обработки и передачи информации.

Список литературы

[1] Грибунин, Вадим Геннадьевич Стеганография, цифровые водные знаки и стеганоанализ / Грибунин Вадим Геннадьевич. - М.: Вузовская книга, 2018. - 110 с.

[2] Земцов, Андрей Методы цифровой стеганографии для защиты авторских прав: моногр. / Андрей Земцов. - М.: LAP Lambert Academic Publishing, 2019. - 148 с.

[3] Рассел, Джесси Стеганография / Джесси Рассел. - М.: VSD, 2019. - 193 с.

[4] Рябко, Б. Я. Основы современной криптографии и стеганографии / Б.Я. Рябко, А.Н. Фионов. - М.: Горячая линия - Телеком, **2019**. - 232 с.

[5] Рябко, Борис Яковлевич Основы современной криптографии и стеганографии / Рябко Борис Яковлевич. - М.: Горячая линия - Телеком, **2019**. - **166** с.

[6] Орлов Д. В., Нестеренков, С. Н., Марков А.Н., Сравнительный анализ методов бинаризации изображений [Электронный ресурс]URL:https://libeldoc.bsuir.by/handle/123456789/4834

[7] Ситников А.В., Нестеренков С.Н., Марков А.Н. Методы защиты больших данных [Электронный ресурс]. URL: https://libeldoc.bsuir.by/handle/123456789/48384.

QUALITY EVALUATION OF INFORMATION TRANSFER IN A DISPATCHING SYSTEM BASED ON MQTT ARCHITECTURE

I.V. Losik
Student of the Faculty of Computer Systems and Networks

S.N. Nesterenkov
Dean of the Faculty of Computer Systems and Networks of the Belarusian State University of Informatics and Radioelectronics, Associate Professor of the Department of Software information Technology

D.V. Nizovtsov
Head of Information Technology Department,assistant of the department of Software information Technology

Department of Information and Computer Systems Design
Faculty of Computer Systems and Networks
Belarusian State University of computer science and Radio Electronics, Republic of Belarus
E-mail: alexvikt.minsk@gmail.com

Annotation. In this paper, the principles of steganographic methods, various algorithms for hiding information and tools for their detection were considered. The topic of the relevance of the development of steganography methods and tools for their detection in the field of cybersecurity was also raised. Understanding steganographic techniques and applying them can help protect data from unauthorized access and keep personal information private.

Keywords: Steganography, LSB, cryptography, cybersecurity.