УДК 159.99

СТЕГАНОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Вилкина К. А., студент гр.253504, Клебеко Е. Ю., студент гр.253504
Носкович П. Н., студент гр.253504

Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь

Стройникова Е. Д. – ст. преп. кафедры информатики

Аннотация. В данной статье были рассмотрены методы защиты информации с использованием стеганографии, а также предложен вариант реализации метода стеганографии с наименьшим значащим битом.

Ключевые слова. Стеганография, стеганографические методы, сокрытие информации

Стеганография — это средство сокрытия секретной информации внутри обычного, несекретного документа или другого носителя, чтобы избежать обнаружения. Произошло от греческого steganos и graphy, что вместе означает “тайнопись” или “скрытое письмо”.

Стеганография и криптография преследуют одну и ту же цель — защитить сообщение или информацию от третьих лиц, но в отличие от криптографии, в стеганографии скрытым является сам факт передачи информации.

При использовании стеганографических методов защита информации происходит на трех уровнях:

1. Неизвестен сам факт передачи скрытой информации;
2. Неизвестен алгоритм помещения скрытой информации в контейнер (под контейнером подразумевается открытый текст, где скрыта зашифрованная информация);
3. Неизвестен способ кодирования информации.

Один из наиболее распространенных методов называется стеганографией с наименьшим значащим битом (LSB — least significant bit). Это включает в себя встраивание секретной информации в младшие значащие биты медиафайла. К примеру, изменение последнего бита значения пикселя не приводит к визуально заметному изменению изображения, а это означает, что никто не сможет отличить исходное изображение от стеганографически модифицированного.

Ниже представлен вариант реализации данного метода на базе языка Python с использованием библиотеки steganocryptopy. В результате активации данного кода, мы получаем ещё одну фотографию, которая внешне ничем не отличается от первоначального варианта, разница будет только в их размер, и то она минимальна. В дальнейшем, используя заранее сгенерированный ключ (строка 3), мы можем дешифровать сообщение.

```
1  from steganocryptopy.steganography import Steganography
2
3  Steganography.generate_key("")
4  secret = Steganography.encrypt("key.key", "C:/Users/VAG/Desktop/img/lisi4ka.png"
       , "secrettext.txt")
5  secret.save("C:/Users/VAG/Desktop/img/lisi4ka_secret.png")
6  result = Steganography.decrypt("key.key", "C:/Users/VAG/Desktop/img
       /lisi4ka_secret.png")
7  print(result)
```

Рисунок 1 - Реализация метода стенографии с наименьшим значащим битом

Этот же метод может быть применен к другим цифровым носителям, таким как аудио и видео, где данные скрыты в частях файла, что приводит к наименьшим изменениям в звуковом или визуальном выводе.

Различают 5 видов стеганографии: стеганография изображений, текстовая, видео, аудио и сетевая стеганографии.

Стеганография изображений.

Включает в себя сокрытие информации в файлах изображений. Интенсивность пикселей является ключом к сокрытию данных в стеганографии изображений. В цифровой стеганографии изображения часто используются для сокрытия информации, поскольку в цифровом представлении

изображения имеется большое количество элементов, и существуют различные способы сокрытия информации внутри изображения.

Текстовая стеганография.

Текстовая стеганография предполагает сокрытие информации внутри текстовых файлов. В этом методе скрытые данные кодируются буквой каждого слова. Метод также включает в себя изменение слов в тексте, использование контекстно-свободных грамматик для создания читаемых текстов или создание случайных последовательностей символов.

Видео стеганография.

Именно здесь данные скрываются в форматах цифрового видео. Видео стеганография позволяет скрывать большие объемы данных в движущемся потоке изображений и звуков. Дискретное косинусное преобразование (DCT) обычно используется для вставки значений, которые можно использовать для сокрытия данных в каждом изображении в видео, что невозможно обнаружить невооруженным глазом.

Аудио стеганография.

Аудио стеганография — это сокрытие данных в звуке. Она включает в себя секретные сообщения, встраиваемые в звуковой сигнал, который изменяет двоичную последовательность соответствующего звукового файла. Сокрытие секретных сообщений в цифровом звуке — более сложный процесс по сравнению с другими.

Сетевая (протокольная) стеганография.

Сетевая стеганография, иногда называемая стеганографией протокола, представляет собой метод встраивания информации в протоколы управления сетью, используемые при передаче данных, такие как TCP (Transmission Control Protocol), UDP (User Datagram Protocol), ICMP (Internet Control Message Protocol) и т. д. Типичные методы сетевой стеганографии включают изменение свойств одного из сетевых протоколов.

К примерам стеганографии можно отнести:

- Написание невидимыми чернилами.
- Встраивание текста в изображение (водяные знаки).
- Обратную запись сообщения в аудиофайле.
- Скрытие изображения в видео, которое можно увидеть, только если видео воспроизводится с определенной частотой кадров.
- Встраивание секретного сообщения в зеленый, синий или красный каналы изображения RGB.

Стеганографию можно использовать как в конструктивных, так и в деструктивных целях. Например, для создания авторами изображений невидимых водяных знаков. Последние не искажают изображение и при этом позволяют отслеживать, использовалось ли оно без разрешения.

Однако, с другой стороны, хакеры используют стеганографию для повреждения файлов, данных или сокрытия вредоносных программ в невинных документах. Например, злоумышленники могут использовать скрипты BASH и PowerShell для запуска автоматических атак, встраивая скрипты в документы Word или Excel. И когда пользователь открывает один из этих документов, он активирует скрытый сценарий, тем самым давая волю вредоносным программам. Этот процесс является предпочтительным методом доставки программ-вымогателей.

Практика обнаружения стеганографии называется стегоанализом. Существуют различные инструменты, способные обнаруживать наличие скрытых данных, например StegExpose и StegAlyze. Аналитики могут использовать другие инструменты общего анализа, такие как программы просмотра шестнадцатеричных файлов, для обнаружения аномалий в файлах.

Однако стоит отметить, что поиск файлов, которые были изменены с помощью стеганографии, является сложной задачей потому, что практически невозможно узнать, где начать искать скрытые данные среди миллионов изображений, загружаемых в социальные сети каждый день.

Список использованных источников:

1. kaspersky / What is steganography? Definition and explanation [Электронный ресурс] – kaspersky – 2023. – Режим доступа : https://www.kaspersky.com/resource-center/definitions/what-is-steganography / Дата доступа: 10.04.2023.

2. simplilearn / What is Steganography? Types, Techniques, Examples & Applications [Электронный ресурс] – simplilearn – 2023. – Режим доступа : https://www.simplilearn.com/what-is-steganography-article / Дата доступа: 10.04.2023.

UDC 159.99

STEGANOGRAPHIC METHODS OF INFORMATION PROTECTION

Vilkina. K. A., Klebeko E. Y., Noskovich P. N.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Stroinikova E. D. – Senior Lecturer in Department of Informatics

Annotation. In this article, methods for protecting information using steganography were considered, and a variant of implementing the steganography method with the least significant bit was proposed.

Keywords: steganography, steganographic methods, information hiding