ПРИМЕНЕНИЕ СТЕГАНОГРАФИИ В КОМПЬЮТЕРНЫХ АТАКАХ

Станчук П.Н.

Станчук Полина Николаевна – студент,
кафедра управление и защита информации,
Российский университет транспорта, г. Москва

Аннотация: *в статье рассмотрено применение стеганографических методов встраивания информации в изображение при проведении компьютерных атак*
Ключевые слова: *информационная безопасность, стеганография, алгоритм Коха-Жао, встраивание информации, компьютерная атака*

USE OF STEGANOGRAPHY IN COMPUTER ATTACKS

Stanchuk P.N.

Stanchuk Polina Nikolaevna – Student,
DEPARTMENT OF INFORMATION MANAGEMENT AND PROTECTION,
RUSSIAN UNIVERSITY OF TRANSPORT, MOSCOW

Abstract: *the article considers the use of steganographic methods of embedding information in an image during computer attacks*
Keywords: *information security, steganography, Koch-Zhao algorithm, information embedding, computer attack.*

УДК 331.225.3

Стеганография — это способ спрятать информацию внутри другой информации или физического объекта так, чтобы ее нельзя было обнаружить, то есть скрывается сам факт передачи информации. С помощью стеганографии можно спрятать практически любой цифровой контент, включая тексты, изображения, аудио- и видеофайлы. При поступлении спрятанной информации к адресату её извлекают [1].

Выделяют следующие виды стеганографии:

- текстовая (встраивание информации в текстовые файлы);
- сетевая (встраивание информации в сетевые протоколы, используемые при передаче данных);
- в изображениях (встраивание информации в графические файлы);
- в видео (встраивание информации в цифровые видеоформаты);
- в звуке (встраивание информации в аудиосигнал) [1].

Целями применения стеганографии являются:

- сокрытие факта передачи информации;
- подтверждение подлинности предаваемых данных;
- скрытая аннотация и аутентификация передаваемой информации [2].

Методы стеганографии используются для проведения компьютерных атак. Например, исследователи компании Check Point в 2016 году обнаружили новый вектор атак, названный ImageGate. Злоумышленники внедряли вредоносный код в изображения и графические файлы. Код на изображениях выполнялся через приложения социальных сетей. При загрузке и открытии полученного вредоносного файла пользователем, все файлы на персональном устройстве автоматически шифровались, и они могли получить к ним доступ только после уплаты выкупа [3].

В 2022 году исследователи из Symantec Enterprise обнаружили троянский бэкдор, использующий стеганографию. Загрузчик DLL загружал растровый файл логотипа Microsoft Windows из репозитория GitHub. Полезная нагрузка представляла собой полнофункциональный бэкдор, была скрыта в файле и расшифровывалась с помощью ключа XOR.

Маскировка полезной нагрузки таким образом позволила злоумышленникам разместить вредоносный файл на бесплатном надежном сервисе. Загрузка с надежных хостов с гораздо меньшей вероятностью вызовет тревогу, чем загрузка с сервера, контролируемого злоумышленником [4].

Выделяют следующие причины проведения компьютерных атак с применением стеганографии:

- сокрытие самого факта загрузки и выгрузки данных;
- обход систем глубокого анализа трафика (DPI-систем);
- обход проверки в системах раннего выявления сложных угроз (AntiAPT-системах) [5].

Рассмотрим один из методов встраивания информации в изображение. Метод стеганографического встраивания Коха–Жао использует двумерное дискретное косинусное преобразование.

Алгоритм:

1) Разбиение исходного изображения на блоки размером 8 × 8 пикселей.
2) Применение дискретного косинусного преобразования к каждому блоку. Получение набора матриц коэффициентов Di (i = 1, ..., N; N — количество блоков) размером 8 × 8.
3) Выбор блоков для встраивания. Запись в каждый выбранный блок по 1 биту информации.
4) Выбор в каждом блоке по 2 коэффициента дискретного косинусного преобразования, симметричных относительно главной диагонали.
5) Для встраивания нулевого бита разность модулей пары коэффициентов дискретного косинусного преобразования должна превышать пороговое значение M_0, для встраивания единичного бита разность должна быть меньше M_0.

Формула вычисления абсолютных значений данных разностей для всех блоков изображения:

$$C_i = \left| |D_i(k_1, k_2)| - |D_i(k_2, k_1)| \right|,$$

где $D_i(x, y)$ – значение коэффициента дискретного косинусного преобразования с индексами (x, y) в i-м блоке

6) Выполнение пунктов 4 и 5 для каждого блока.
7) Выполнение обратного дискретного косинусного преобразования для каждого блока [6].

Встраивание в низкочастотные компоненты изменяет фон изображения, в высокочастное — искажает мелкие детали. Оптимально производить встраивание в среднечастотные компоненты, так как такой метод встраивания позволяет минимизировать искажения [6].

Рассмотрим пример встраивания сообщения в изображение при помощи алгоритма Коха-Жао. Исходное изображение приведено на рисунке 1.

Рис. 1. Исходное изображение.
Источник: фотография автора.

Программа, реализующая алгоритм, написана на языке Python. В изображение формата jpeg было встроено сообщение:
1111111111111111112222222222222222222223333333333333333344444444aaaaaaaaaaaaaaaaabbbbbbbbb
bbbbbbbbbbccccccccccccccccccccceeeeeeeeeeeeeeeeeeeeeee777777777777777777777777777ababababababa
bbababbababbababbababababdedededededededededegggggggegegegegeggegegegeg555555555555555555555

555555555555555558888888888888888888888888888888855555555555555555555555555555558888888888888888888. Изображение со встроенным текстом приведено на рисунке 2.

Рис. 2. Изображение со встроенным сообщением.
Источник: обработанная фотография автора.

При помощи программы Beyond Compare, позволяющей сравнивать данные, сопоставим исходное изображение с изображением со встроенным сообщением. Значение параметра tolerance равно 25. Результат сравнения представлен на рисунке 3. Красным цветом указаны различия меду исходным изображением и изображением со встроенным сообщением.

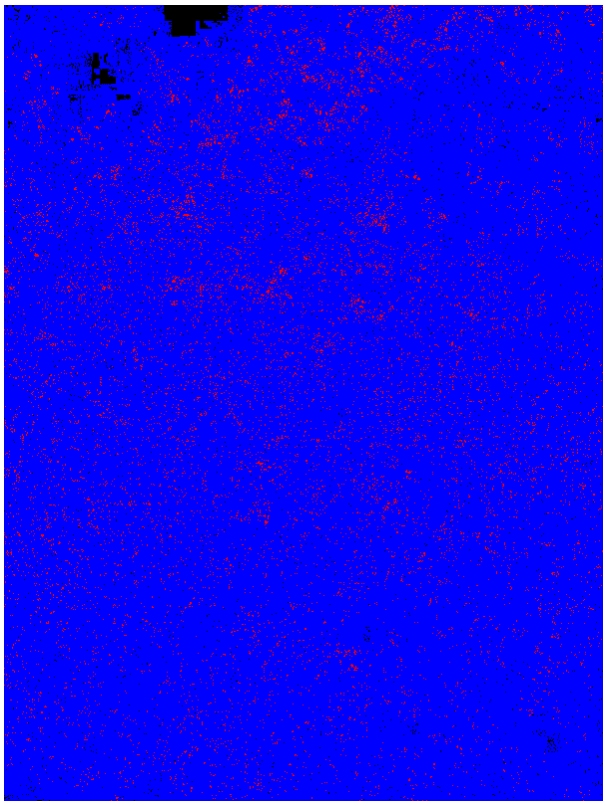

Рис. 3. Результат сравнения изображений.
Источник: сравнение фотографии автора с обработанной фотографией автора при помощи программы Beyond Compare.

Практическая реализация одного из стеганографических алгоритмов встраивания информации в изображение и последующий анализ полученного изображения позволили показать, что данный метод встраивания информации позволяет скрыть от человека сам факт встраивания сообщения в изображение.

Таким образом, необходимо продолжать разработки средств нейтрализации угроз, связанных с компьютерными атаками с использованием методов стеганографии.

Список литературы/ References

1. Что такое стеганография? Определение и описание // kaspersky [Электронный ресурс]. Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-steganography/ (дата обращения: 14.06.2023).
2. АКТУАЛЬНОСТЬ СТЕГАНОГРАФИИ И ЕЕ ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ // elibrary [Электронный ресурс]. Режим доступа: https://www.elibrary.ru/item.asp?id=41880024/ (дата обращения: 14.06.2023).
3. ImageGate: Check Point uncovers a new method for distributing malware through images // Check Point [Электронный ресурс]. Режим доступа: https://blog.checkpoint.com/research/imagegate-check-point-uncovers-new-method-distributing-malware-images/ (дата обращения: 14.06.2023).
4. Witchetty: Group Uses Updated Toolset in Attacks on Governments in Middle East // Symantec by Broadcom [Электронный ресурс]. Режим доступа: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/witchetty-steganography-espionage/ (дата обращения: 14.06.2023).
5. Стеганография в современных кибератаках // Securelist by kaspersky [Электронный ресурс]. Режим доступа: https://securelist.ru/steganography-in-contemporary-cyberattacks/79090/ (дата обращения: 14.06.2023).
6. Стеганоанализ алгоритма Коха-Жао // Cyberleninka [Электронный ресурс]. Режим доступа: https://cyberleninka.ru/article/n/steganoanaliz-algoritma-koha-zhao/ (дата обращения: 14.06.2023).