Telegram-бот для обработки стеганографии в PNG-файлах

Латанов К.В., СГУ, Саратов latanov.kirill@yandex.ru,
Благов М.В., СПбГУ, Санкт-Петербург m.blagov@spbu.ru,
Кузнецов Н.В., СПбГУ, Санкт-Петербург n.v.kuznetsov@spbu.ru

Аннотация

В статье рассматривается метод стеганографического кодирования информации в изображениях формата PNG (Portable Network Graphics), который позволяет встраивать секретные текстовые данные в цифровые изображения без видимого ухудшения их качества и потери целостности. В работе описан алгоритм встраивания и извлечения информации при помощи метода наименее значащих бит (LSB), и Telegram-бот, разработанный с использованием языка программирования Python. Помимо основных стеганографических методов, для усиления защиты бот предоставляет три криптографических метода – шифр Виженера, «Кузнечик» и DES.

Введение

Стеганография необходима для конфиденциальной передачи информации, поскольку она позволяет встраивать скрытые данные в безобидные на первый взгляд файлы, такие как изображения, аудио или видео [1]. Эта техника скрывает сам факт передачи секретной информации, что делает ее идеальным инструментом для обхода систем мониторинга. Стеганографические методы также обеспечивают защиту данных от перехвата, что делает их незаменимыми в условиях современных угроз информационной безопасности. Наличие криптографического шифра не всегда гарантирует защиту, а зашифрованное сообщение нередко выглядит неестественно и привлекает внимание. Поэтому совокупность средств и методов стеганографии и криптографии может обеспечить более надёжный канал коммуникации, который для прочтения сообщения необходимо не только взломать, но и обнаружить сам факт передачи [2].

Теоретическая часть и описание бота

Поскольку внедрение информации будет происходить в нефизический объект, то речь в данной статье пойдёт о цифровой стеганографии.

Цифровая стеганография – ответвление стеганографии, суть которой заключается во встраивании добавочной информации в цифровые объекты. Основными принципами цифровой стеганографии являются изменение объекта без утраты возможности их функционирования и неспособность при помощи органов чувств заметить незначительные искажения в сравнении с оригиналом [3].

В этой работе в качестве цифрового контейнера используется изображение в формате PNG. Выбор данного формата обусловлен рядом преимуществ последнего: широкое использование, поддержка различных глубин цвета, поддержка прозрачности, сжатие без потерь, поддержка метаданных [4].

В качестве усиления защиты используются криптографические средства – шифры Виженера, «Кузнечик» [5] и DES [6]. Первый метод выбран в качестве демонстрационного, поскольку прост в реализации и легок в понимании – шифр Виженера является модификацией шифра Цезаря, который, в свою очередь, является моноалфавитным шифром простой подстановки, где каждая буква исходного сообщения, согласно определённому правилу сдвига, заменяется другой буквой этого же алфавита. Два других метода криптографической защиты являются более надёжными и относятся к блочным симметричным шифрам, каждый из которых в своём алгоритме содержит раундовые преобразования.

В качестве платформы для реализации был выбран Telegram, поскольку большинство коммуникаций в современных реалиях проходят в мессенджерах, а данный представитель является одним из самых популярных [7] и обладает удобными средствами для разработки [8].

Техническая реализация

Описание функционала и демонстрация работы бота

Телеграм-бот написан на языке Python при помощи библиотеки aiogram [9]. Поскольку мессенджер уже имеет свой интерфейс, то дополнительная разработка по части UI не требуется, достаточно только добавления обработчика ввода и сообщений.

При запуске бота пользователю предоставляется выбор – выполнять внедрение или извлечение сообщения из контейнера. После этого выбирается способ шифрования (если текст шифровать не требуется, достаточно выбрать поле «Не шифровать» в контекстном меню) (см. Рис. 1), и в случае выбора такового запрашиваются необходимые для дальнейшего алгоритма параметры, такие как открытые ключи, сдвиг и т. п. На последней стадии

остаётся загрузить контейнер для внедрения, который обязательно должен быть изображением в формате PNG (см. Рис. 2). На случай некорректного ввода на каком-то из шагов предусмотрена обработка состояния с возвращением на предыдущий шаг.

Рис. 1: Процесс подготовки сообщения к внедрению.

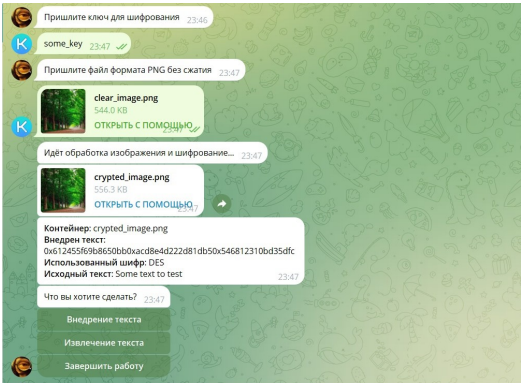

Рис. 2: Процесс внедрения сообщения в изображение.

Процесс извлечения сообщения из контейнера с опциональным расшифрованием выполняется в обратной последовательности – пользователем в меню выбирается опция извлечения, после чего присылается контейнер с встроенным в него сообщением (см. Рис. 3). Далее выбирается поле шифра (если шифрование не применялось, то необходимо указать «Без шифра»), и при необходимости запрашиваются требуемые параметры. В результате на по-

следнем шаге работы программы пользователю выводится исходный текст сообщения, внедрённого в контейнер (см. Рис. 4).

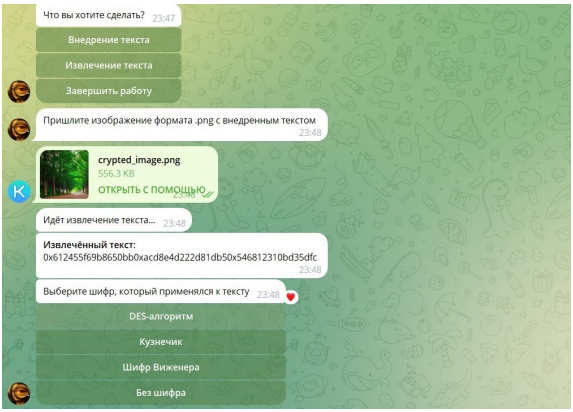

Рис. 3: Процесс получения сообщения из изображения.

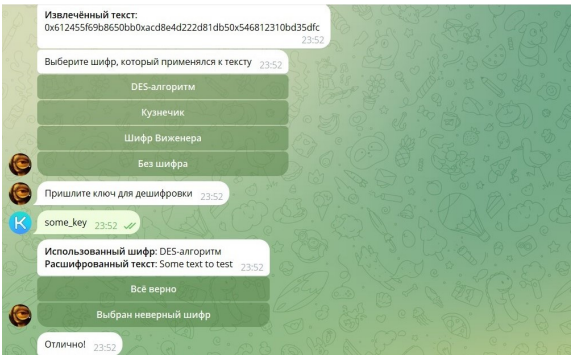

Рис. 4: Процесс получения исходного текста из контейнера.

Заключение

В данной работе была рассмотрена стеганосистема, состоящая из контейнера с изображением в формате PNG, в который встраивается текстовое сообщение. Путём дополнительной обработки перед внедрением можно уси-

лить защиту канала связи, воспользовавшись одним из трёх методов криптографической защиты – шифром Виженера, «Кузнечик» или DES [10].

В качестве платформы для реализации стеганосистемы был выбран Telegram, поскольку данный мессенджер является весьма востребованным, имеет удобный инструментарий для взаимодействия и разработки, а также привычный пользователю интерфейс.

Список литературы

[1] Семененко, В. А. Информационная безопасность: учебное пособие для вузов / В. А. Семененко. – 2-е изд. – Москва: МГИУ, 2005. – 215 с.

[2] Рябко Б.Я. Основы современной криптографии и стеганографии. М.: Горячая линия – Телеком, 2013. 232 с

[3] Грибунин В.Г. Цифровая стеганография. М.: «Солон-пресс», 2020. 262 с

[4] PNG: особенности формата, преимущества и применение в компьютерной графике https://nauchniestati.ru/spravka/png

[5] Бабенко Л.К., Ищукова Е.А., Толоманенко Е.А. Дифференциальный анализ шифра «Кузнечик». Известия ЮФУ. Технические науки. 2017 г.

[6] Paar C., Pelzl J. Understanding Cryptography: A Textbook for Students and Practitioners . Springer, 2009. 390 с.

[7] Популярность мессенджеров в 2024-м: как они будут развиваться https://mindbox.ru/journal/education/populyarnye-messendzheri/

[8] 14 best Python Telegram Bot libraries in 2024 https://kandi.openweaver.com/collections/python/python-telegram-bot

[9] Знакомство с aiogram https://mastergroosha.github.io/aiogram-3-guide/quickstart/

[10] Латанов К.В. Стеганография в графических файлах. Выпускная квалификационная работа, 2024, Саратовский государственный университет, 2024.