DOI 10.36074/logos-23.06.2023.39

ТЕЛЕГРАМ-БОТ, ЩО ВИКОРИСТОВУЄ СТЕГАНОГРАФІЧНІ АЛГОРИТМИ ДЛЯ ПРИХОВУВАННЯ ІНФОРМАЦІЇ В ЦИФРОВИХ ЗОБРАЖЕННЯХ

Коршенко Владислав
Студент,
дипломник 1-го курсу магістратури
Факультет комп'ютерних наук
кафедра безпеки інформаційних систем і технологій
Харківський національний університет імені В. Н. Каразіна

Громико Ігор Олексійович
Керівник проекту,
професор кафедри безпеки інформаційних систем і технологій,
кандидат технічних наук, доцент
Факультет комп'ютерних наук
кафедра безпеки інформаційних систем і технологій
Харківський національний університет імені В. Н. Каразіна

УКРАЇНА

Анотація. *У даній статті представлено результати роботи над проектом "Телеграм-бот, що використовує стеганографічні алгоритми для приховування інформації в цифрових зображеннях". Описано аналіз існуючих рішень у галузі стеганографії та обґрунтовано вибір платформи Телеграм для реалізації проекту. Описано основні функції та можливості розробленого телеграм-боту, включаючи процес приховування та вилучення повідомлень з зображень. Також зазначено обмеження поточної версії телеграм-боту та перспективи подальшого розвитку програмного забезпечення. Керівник проекту ознайомив зі змістом роботи працівників силових структур держави в частині корисних елементів. Робота визнана корисною.*

1. Вступ.

Кібербезпека є однією з найважливіших сфер сучасного світу, яка стає все більш актуальною в контексті військових операцій. Вона необхідна не лише для боротьби з хакерами та кіберзлочинцями, але й для досягнення перемоги в збройних конфліктах. З відкритих програм телебачення прозвучало, що і Збройні Сили України (ЗСУ), і ворожі сили використовують однотипні прилади зв'язку, що створені на заводах західної Європи. Станом на даний момент, деякі «польові» радіостанції для ЗСУ, держава-агресор може вільно придбати через фірми-прокладки. Це вказує на те, що обидві сторони можуть прослуховувати один одного, що створює серйозні потенційні загрози для безпеки військової інформації.

Саме тому поява закритих (захищених) каналів зв'язку, до яких не мають доступу ворожі сили, стає важливим завданням. Створення таких каналів зв'язку є надзвичайно актуальною проблемою, яка вимагає розробки нових технологій та підходів. Один із потенційних методів вирішення цієї проблеми полягає в застосуванні стеганографічних алгоритмів для приховування інформації в цифрових зображеннях.

Метою даної магістерської роботи є розробка та створення телеграм-боту, який використовує стеганографічні алгоритми з метою приховування інформації в цифрових зображеннях. Основний сенс роботи полягає у створенні ефективного програмного застосунку, що забезпечує конфіденційність передачі інформації та є простим і зручним у користуванні. Результати цього дослідження можуть мати велике значення для забезпечення безпеки комунікаційних систем, а також для підвищення їх ефективності в умовах сучасних кіберзагроз.

2. Методи.

2.1 Аналіз існуючих рішень

У процесі аналізу існуючих програмних рішень для стеганографічного приховування інформації в зображеннях з метою організації закритих каналів зв'язку, було виявлено ряд програм, що вирішують цю проблему, але з обмеженою ефективністю та функціональністю.

Одним зі способів приховування інформації в зображеннях є використання спеціалізованих сайтів, які дозволяють приховати текстові повідомлення в цифрових зображеннях. Такі рішення частково вирішують проблему стеганографії, але вони мають свої обмеження та недоліки. Один із головних недоліків полягає у необхідності використання довільних каналів зв'язку для передачі зображення із прихованим повідомленням. Це створює певний ризик виявлення і перехоплення даного повідомлення.

2.2 Опис вимог

У процесі розробки телеграм-боту були встановлені основні критерії для вибору програмних рішень. Ці критерії враховували вимоги до безпеки та простоти користування.

Першим і найважливішим критерієм була конфіденційність передачі інформації. Приховування даних в зображеннях повинно забезпечувати високий рівень безпеки та недоступність для сторонніх осіб.

Другим критерієм була анонімність користувачів. Застосунок повинен забезпечувати можливість взаємодії між користувачами без необхідності розголошувати їх особисту інформацію.

Третім критерієм була криптостійкість. Алгоритми, що використовуються для обміну повідомленнями, мають бути стійкими до розшифрування та атак з боку противника.

Нарешті, останнім критерієм була простота користування. Розроблений програмний застосунок повинен бути легким у використанні, навіть для недосвідчених користувачів, щоб забезпечити зручну і ефективну комунікацію.

З урахуванням вищезазначених критеріїв, було прийнято рішення про використання месенджеру Телеграм, як платформи для розробки боту. Цей вибір був обґрунтований низкою факторів, що позитивно впливають на захищеність даних та анонімність користувачів.

По-перше, Телеграм використовує криптографічний протокол MTProto для забезпечення конфіденційності передачі даних. Крім того, месенджер має відкритий вихідний код API (прикладного програмного інтерфейсу), що дозволяє розробникам створювати безпечні програмні рішення для комунікації.

По-друге, практика показала, що більшість військових використовують смартфони для обміну тактичною та особистою інформацією, зокрема у месенджері Телеграм. Враховуючи цей факт, створення боту на цій самій платформі усуває необхідність завантаження стороннього програмного забезпечення та час, що зазвичай потрібен для його освоєння.

Стеганографічні алгоритми, що лягли в основу алгоритму, були розглянуті у рамках дисципліни, що викладав видатний вчений України Кузнецов О.О.

2.3 Опис програмних рішень

Програмна реалізація була виконана мовою програмування Java з використанням фреймворку Spring. Ця комбінація дозволяє ефективно створювати додатки з мікросервесною архітектурою. Обрана архітектура дозволяє в майбутніх версіях ПЗ винести стеганографічні алгоритми в окремий мікросервис. Це може бути корисним при потребі в розміщені стеганографічного шифратора та дешифратора на окремому сервері в цілях створення додаткового шару безпеки.

Для взаємодії ПЗ і месенджеру Телеграм був використаний TelegramBotsAPI – прикладний програмний інтерфейс, що створений розробниками самого месенджеру. Цей інтерфейс містить програмні методи, що дозволяють налагодити прийом даних від користувача, а саме вибір режиму роботи ПЗ, текст для приховування, зображення-контейнер, та відправку зворотних даних, таких, як список доступних дій, зображення-контейнер із прихованим текстом, повідомлення про помилку.

Для розгортання ПЗ на сервері була використана система контейнеризації Docker, що дозволяє суттєво спростити сам процес розгортання.

Важливою перевагою створеного програмного застосунку є те, що процеси приховування і вилучення повідомлення відбуваються на одному сервері, де розміщений бот, а не є окремим додатком, що потрібно завантажувати на смартфон. Таким чином алгоритм приховування інформації доступний лише на цьому сервері, що унеможливлює використання реверс-інжинірингу для аналізу вихідного коду застосунку.

В процесі комунікації користувача із ПЗ, дані рухаються наступним ланцюжком:

А) Від користувача на сервер Телеграм;

Б) із серверу Телеграм на сервер з розгорнутим ПЗ;

В момент виконання як кроку А, так і кроку Б, дані користувача захищені протоколом MTProto, а отже передаються у зашифрованому вигляді.

Додатковим шаром безпеки є те, що передача даних відбувається не відразу на сервер ПЗ, а через проміжний сервер самого месенджеру Телеграм. Це заважає потенційним зловмисникам дізнатись IP адресу серверу, на якому працює стеганографічний шифратор та дешифратор у складі ПЗ.

2.4 Опис стеганографічних рішень

У створеній версії ПЗ, використовується класичний стеганографічний алгоритм LSB (Least Significant Bit). Його суть полягає у використанні найменш значущих бітів кольорів пікселів зображення.

При використанні кодування кольору пікселя за схемою RGB, яскравість кожної кольорової компоненти загального кольору приймає значення від 0 до 255. Якщо перевести відповідне значення в двійкову систему можна побачити, що максимально можлива кількість розрядів числа дорівнює 8. Алгоритм LSB змінює лише один або два останніх біти, що в результаті дає зміну яскравості або самого кольору в межах 3-4%. Така зміна непомітна оку людини.

Перевагами цього алгоритму є простота реалізації, вкрай низька вірогідність візуального детектування змін зображення та великий об’єм даних на контейнер.

Недоліками використаного алгоритму є вразливість до детектування повідомлення та геометричних атак (стискання, зміна орієнтації зображення).

Причиною цих недоліків є те, що алгоритм LSB приховує інформацію у просторовій області зображення.

В наступній версії ПЗ буде використано алгоритм Куттер-Джордана-Боссена, що приховує інформацію в частотній області зображення. Такий підхід дозволить захистити дані від геометричних атак, підвищить стійкість до детектування повідомлення та дасть можливість працювати з різними форматами зображень.

3. Результати.

Результати роботи над проектом під назвою "Телеграм-бот, що використовує стеганографічні алгоритми для приховування інформації в цифрових зображеннях" дозволили створити функціональний телеграм-бот. Його основна мета полягає в можливості приховування текстової інформації в зображеннях з подальшим їх використанням для безпечної комунікації в месенджері Телеграм.

Користувачеві надається зручний інтерфейс, який дозволяє приховати повідомлення всього за кілька простих кроків. Після запуску бота, користувач може обрати опцію "Приховати текст" з головного меню, відправити обране зображення, що стане контейнером для повідомлення, та відправити саме повідомлення. Результатом є зображення з прихованим текстом, яке можна негайно переслати або відправити в потрібний чат у месенджері.

До важливої уваги представляється два зображення.

Рис. 1. **порожнє зображення-контейнер**

Рис. 2. **зображення-контейнер із вкладеним**

Рисунок 1 - не містить жодних текстових повідомлень, а Рисунок №2 містить повний текст гімну України: «Ще не вмерла України ні слава, ні воля. Ще нам, браття молодії, усміхнеться доля. Згинуть наші вороженьки, як роса на сонці, Запанує і ми, браття, у своїй сторонці. Душу й тіло ми положим за нашу свободу, І покажем, що ми, браття, козацького роду».

Як ви бачите, - візуально перше та друге зображення не відрізняються один від одного.

Процес вилучення прихованого повідомлення також відбувається у тому ж боті. Для цього користувач повинен запустити бота, обрати опцію "Вилучити текст" з головного меню і надіслати зображення, що містить приховану інформацію. Результатом буде отримання прихованого повідомлення.

Прототип програмного забезпечення має деякі обмеження в даній версії. Зокрема, алгоритм працює лише з зображеннями у форматі .png і дозволяє приховати до 4096 символів у одному зображенні через технічні обмеження платформи. Однак, ці недоліки будуть виправлені у наступних версіях програмного забезпечення.

4. Обговорення.

Один з аспектів обговорення стосується контекстуальності фотографій, які використовуються як контейнери для приховання повідомлень. Запропоновано, щоб відправлені зображення органічно вписувалися в контекст діалогу. Наприклад, якщо обрано зображення квітів, рекомендується супроводжувати його коментарем, що стосується саме квітів (наприклад: "Подивись, які гарні квіти"). Це допоможе зберегти природність спілкування, що в свою чергу дозволить приховати факт обміну важливою інформацією від третіх осіб навіть у випадку втрати смартфону.

Крім того, для запобігання порушення авторських прав на зображення, рекомендується використовувати фотографії, зроблені самим користувачем за допомогою камери смартфону. Це дозволить уникнути можливих проблем із використанням чужих матеріалів і забезпечить правильне використання зображень у контексті комунікації.

Надалі, вже ведеться розробка наступної версії програмного забезпечення. В цій версії планується вдосконалення стеганографічного алгоритму, що забезпечує стійкість до стиснення файлів. Також, перед вбудовуванням інформації буде застосовуватись шифрування, що підвищує рівень безпеки. У додаток до формату .png, будуть підтримуватись і формат .jpg для забезпечення більшої гнучкості при виборі зображень.

5. Висновки.

Розроблений програмний застосунок забезпечує створення закритих каналів зв'язку з високим рівнем захисту даних та зручною комунікацією для військових та інших користувачів. Використання стеганографічних алгоритмів та месенджеру Телеграм створює надійну основу для приховування інформації в цифрових зображеннях і забезпечує надійну комунікацію, значно зменшуючи ризику виявлення та перехоплення повідомлень.

Це відкриває нові можливості для забезпечення безпеки та приватності комунікації, а також створює підґрунтя для подальших досліджень у галузі стеганографії та кібербезпеки.

Список використаних джерел:

[1] Suri, J. S., Shivani, S., & Agarwal, S. (2018). Handbook of Image-Based Security Techniques. Taylor & Francis Group.

[2] Yahya, A. (2018). Steganography Techniques for Digital Images. Springer.