РАКЕТНО-КОСМИЧЕСКОЕ ПРИБОРОСТРОЕНИЕ И ИНФОРМАЦИОННЫЕ СИСТЕМЫ
2024, том 11, выпуск 3, с. 34–38

СИСТЕМНЫЙ АНАЛИЗ, УПРАВЛЕНИЕ КОСМИЧЕСКИМИ АППАРАТАМИ, ОБРАБОТКА ИНФОРМАЦИИ И СИСТЕМЫ ТЕЛЕМЕТРИИ. ДИСТАНЦИОННОЕ ЗОНДИРОВАНИЕ ЗЕМЛИ

УДК 004.8 EDN KBWGT

Бесконтейнерный метод сокрытия информации с использованием нейронных сетей

М. А. Кудрявцев, *kudryavtsevma@yandex.ru*
МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

Аннотация. С быстрым развитием информационных технологий защита передаваемых данных становится одной из приоритетных задач. Классические методы шифрования эффективно решают эту проблему, однако иногда необходимо скрыть сам факт передачи важной информации. Одним из возможных решений могут быть стеганографические методы, которые скрывают сам факт передачи, добавляя данные в существующие цифровые ресурсы. В научной литературе описано множество традиционных стеганоалгоритмов. В последние годы методы сокрытия информации с помощью нейронных сетей становятся все более популярными [1]. Однако большинство таких методов используют нейронные сети для реализации более сложных функций встраивания данных, не создавая новых способов сокрытия информация. Целью работы является краткий обзор разработанного автором метода сокрытия информации без использования цифровых ресурсов — изображений для встраивания и приведение некоторых критериев оценки его эффективности и надежности. В начале статьи дается описание существующих стеганографических методов, общая структура предложенного метода. Оценивается сходимость предложенного алгоритма, генерирующего равномерно распределенный массив данных, даются временные и емкостные характеристики разработанного метода. Приводятся примеры исходных данных и сгенерированных на их основе изображений.

Ключевые слова: стеганография, сокрытие данных, нейронные сети, генерация изображений, бесконтейнерные методы

Для цитирования: Кудрявцев М. А. Бесконтейнерный метод сокрытия информации с использованием нейронных сетей. *Ракетно-космическое приборостроение и информационные системы*. 2024. Т. 11. № 3. С. 34–38.

Container-Free Method of Hiding Information Using Neural Networks

M. A. Kudryavtsev, *kudryavtsevma@yandex.ru*
Bauman Moscow State Technical University, Moscow, Russian Federation

Abstract. The protection of transmitted data is becoming one of the priorities with the rapid development of information technology. Classical encryption methods effectively solve this problem, however, sometimes it is necessary to hide the very fact of transmitting the important information. One possible solution may be steganographic methods that hide the very fact of transmission by adding data to existing digital resources. Many traditional steganoalgorithms have been described in the scientific literature. In recent years, methods of hiding information using neural networks have become increasingly popular [1]. However, most of these methods use neural networks to implement more complex data embedding functions without creating new ways to hide information. The purpose of the work is a brief overview of the method of hiding information developed by the author without using digital resources – images for embedding and providing some criteria for evaluating its effectiveness and reliability. The paper begins with a description of the existing steganographic methods and the general structure of the proposed method. The convergence of the proposed algorithm generating a uniformly distributed data array is estimated, and the time and capacitance characteristics of the developed method are given. The examples of the source data and images generated based on them are presented.

Keywords: steganography, data hiding, neural networks, image generation, container-free methods

For citation: Kudryavtsev M.A. Container-Free Method of Hiding Information Using Neural Networks. *Rocket-Space Device Engineering and Information Systems*. 2024. Vol. 11. No. 3. P. 34–38.

Введение

Передача информации играет ключевую роль в современном мире, где каждый день осуществляется обмен огромными объемами данных. С ростом цифровизации и глобальной интеграции возрастают и риски, связанные с несанкционированным доступом к информации, ее перехватом и модификацией. В этой связи необходимость защиты информации становится одной из наиболее острых проблем.

Наиболее распространенные средства защиты информации включают криптографию и стеганографию. Криптография, основанная на математических алгоритмах шифрования, обеспечивает конфиденциальность и целостность данных. Тем не менее она имеет ряд существенных недостатков. Во-первых, высокая вычислительная сложность криптографических алгоритмов требует значительных ресурсов, что делает их применение не всегда целесообразным в условиях ограниченных вычислительных мощностей. Во-вторых, существующие методы криптоанализа продолжают развиваться, что ставит под угрозу безопасность даже самых современных криптографических систем.

Стеганография, в свою очередь, предлагает альтернативный подход к защите информации, скрывая сам факт передачи данных [2, 3, 4].

В последнее время набирает популярность стеганография на основе нейронных сетей. Алгоритмы этой группы основаны на использовании глубоких нейронных сетей [5, 6], которые обучаются скрывать информацию в изображениях таким образом, чтобы она была незаметна для человеческого глаза и не поддавалась простому математическому описанию.

Основным недостатком всех рассмотренных стегометодов методов является то, что они используют изображения в качестве контейнера-обложки, что значительно влияет на объем скрываемой информации и выбор алгоритмов для сокрытия. Таким образом, между современными стегометодами основное отличие заключается в подходах к встраиванию сообщения.

Серьезным недостатком современных методов на основе нейронных сетей является невозможность встраивания информации в некоторые изображения (особо большие трудности возникают с очень светлыми и очень темными изображениями). Кроме того, многие методы не дают гарантии успешного встраивания и извлечения скрытого сообщения [7].

В работе [8] автор приводил общий алгоритм работы предложенного метода, в рамках текущей статьи будет приведена общая идея математической модели прямого преобразования байтовой последовательности в изображение.

Математическая модель

Исходное, скрываемое сообщение (Message) может быть выражено в виде конечной байтовой последовательности. Тогда можно сделать предположение, что $Message = \langle x_1, x_2, \ldots, x_N \rangle$ — кортеж, в котором $x_1, x_2, \ldots, x_N$ — элементы из конечного поля $F(256)$, а $N \geqslant 1$ — общее число элементов.

В работе рассматривается преобразование в изображение в формате PNG-48bit в цветовом пространстве RGB. Пусть $H \geqslant 1$ и $W \geqslant 1$ — высота и ширина получаемого изображения в пикселях соответственно. Тогда изображение *Image*, получаемое в результате преобразования, представляется как матрица

$$\begin{pmatrix} rgb_{11} & \ldots & rgb_{1W} \\ \vdots & \ddots & \vdots \\ rgb_{H1} & \ldots & rgb_{HW} \end{pmatrix},$$

где $rgb_{ij} =< r_{ij}, g_{ij}, b_{ij} >\in F(256)2$.

Для преобразования из *Message* в *Image* предлагаемый метод содержит следующие этапы:

1) применение кодов восстановления Рида–Соломона к исходной байтовой последовательности *Message*;
2) генерация равномерно распределенной выборки данных длины H^*W^*3 на основе данных этапа 1;
3) преобразование равномерного распределения в нормальное;
4) применение нейронной сети к данным, полученным на этапе 3;
5) преобразование в PNG-48bit формат.

Отдельное внимание стоит обратить на этапе со второго по четвертый. На втором этапе, на основе входной байтовой последовательности происходит генерация равномерно распределенного массива вещественных значений [8]. Важной особенностью является то, что каждое сгенерированное значение зависит от всей исходной последовательности. Основой этого этапа является модификация линейного конгруэнтного метода. В общем случае такая модификация позволяет получать случайные равномерно распределенные целые числа в заданном диапазоне. Для реализации метода был использован вариант генерации с двумя переменными:

$$x_{i+1} = F(x_i, x_{i-1}) = (ax_{i-1} + bx_i + c) \bmod m;$$

$$z = F(x, y) = (ax + by + c) \bmod m.$$

На третьем и четвертом этапах предложенного метода возможно нарушение целостности данных. Для гарантированного сохранения целостности исходного сообщения были применены коды восстановления Рида–Соломона. Их применение в методе обусловлено необходимостью обработки байтовой последовательности произвольной длины. Для этого входная последовательность делится на блоки фиксированной длины, а для каждого блока вычисляются вспомогательные символы [8].

С ошибками, возникающими на третьем и четвертом этапах, помогают бороться коды восстановления, однако модификация линейного конгруэнтного метода, сделанная на втором этапе, нуждается в проверке. Для этого воспользуемся критерием Колмогорова для оценки согласия.

Проверка работы второго этапа

Целью этапа является преобразование данных в равномерно распределенную последовательность чисел. Пропустим $N = 10000$ входных сообщений длины $M = 100$ через предложенный алгоритм и получим соответственно 10 000 выходных массивов $X_1, \ldots, X_{10\,000}$. Для каждого из них сформулируем основную и альтернативную статистические гипотезы о характере их распределения:

$$H_0: \quad F_{X_i}(x) = R(x)$$

$$H': \quad F_{X_i}(x) \neq R(x),$$

где

$$R(x) = \begin{cases} 0, x < 0 \\ x, 0 \leqslant x < 1 \\ 1, x \geqslant 1 \end{cases}$$

— функция распределения равномерного распределения.

В качестве критерия согласия возьмем критерий Колмогорова, ввиду следующих причин:

1) критерий предназначен для проверки гипотезы о принадлежности выборки некоторому закону распределения (в нашем случае равномерному распределению);
2) для использования критерия необходимо только знать эмпирическую функцию распределения $F^*_{X_i}(x)$, которую можно получить по выборке по определению:

$$F^*_{X_i}(x) = \frac{\text{card}\{x' \in X_i | x' < x\}}{\text{card} X_i}.$$

Статистика критерия Колмогорова:

$Z_n = \sqrt{n} D_n \sim K$ имеет распределение Колмогорова, где

$$D_n = \Delta(F^*_{X_i}(x),\ \ R(X)) = \sup_{x \in X_i} |F^*_{X_i}(x) - R(x)|.$$

При уровне доверия $\alpha = 0{,}95$ имеем квантиль распределения Колмогорова $z_{1-\alpha} = z_{0{,}05} \simeq 1{,}36$. Соответственно при $Z_n < z_{1-\alpha}$ гипотеза H_0 отвергается.

В ходе эмпирических исследований выяснилось, что для 70 000 случайных входных сообщений гипотеза H_0 принялась в 58 917 случаях (84,17 %).

При уровне доверия $\alpha = 0{,}995$ (квантиль распределения Колмогорова $z_{1-\alpha} = z_{0{,}005} \simeq 1{,}73$) гипотеза принялась в 67 376 случаях из 70 000 (96,25 %).

При уровне доверия $\alpha = 0{,}9$ (квантиль распределения Колмогорова $z_{1-\alpha} = z_{0{,}1} \simeq 1{,}63$) гипотеза принялась в 66 051 случаях из 70 000 (94,36 %).

Таким образом, был проведен анализ предложенной функции для генерации равномерно распределенной последовательности, зависящей от двух переменных.

Производительность разработанного алгоритма

Разработанный метод реализован и протестирован на домашнем компьютере и мобильном телефоне. Размер скрываемой информации — 108 000 байт.

Характеристики компьютера:

операционная система — Ubuntu 20.04 LTS,

процессор — Intel Core i5-9600K,

видеокарта — MSI GeForce GTX 1650 SUPER,

модель мобильного устройства — Poco F4 (6/128).

В таблице представлено среднее время выполнения для каждого устройства при 1000 запусках.

Таблица. Сравнение времени работы алгоритма на устройствах

Использованное устройство	Время работы модели, мс	Общее время кодирования, мс	Общее время декодирования, мс
Компьютер (процессор)	130	198	224
Компьютер (видеопамять)	57	136	158
Мобильное устройство (процессор)	478	653	649

Примеры работы алгоритма

Для демонстрации работы алгоритма скроем три сообщения:

1. Текстовое (аннотация статьи).

2. Байтовую последовательность (случайных набор байт размером 98 кб).

3. Документ в формате docx.

Сгенерированные изображения представлены на рисунке.

Рисунок. Изображения, сгенерированные на основе входящих сообщений

Figure. The images generated based on incoming messages

Заключение

В статье рассмотрен алгоритм сокрытия информации в изображениях, позволяющий исключить необходимость использования изображений-обложек для встраивания информации, исключая тем самым наиболее уязвимое место любого стего-алгоритма. Предложенный метод работает с одним из самых популярных форматов изображений — PNG и способен работать как на компьютерах, так и на мобильных устройствах, обеспечивая достаточно высокую производительность для общения в режиме реального времени.

Список литературы

1. *Рудаков И.В.*, *Филиппов М.В.*, *Кудрявцев М.А.* Метод генерации изображений с использованием нейронных сетей на основе восстанавливаемой байтовой последовательности. Вестник МГТУ им. Н.Э. Баумана. Сер. приборостроение, 2023, № 1 (142), С. 83–97.

2. *Nashat D.*, *Mamdouh L.* An efficient steganographic technique for hiding data. Journal of the Egyptian Mathematical Society, 2019.

3. *Kaur H.*, *Jyoti Ran.* A Survey on different techniques of steganography. MATEC Web of Conference ICAET, 2016.

4. *Soumyendu Das*, *Subhendu Das*, *Bijoy Bandyopadhya*, *Sugata Sanya*. Steganography and Steganalysis: Different Approaches. axRiv, 2011.
5. *Bann M*. stegoVeritas // Веб-сайт GitHub, Inc. 2021. https://github.com/bannsec/stegoVeritas
6. *Lerch-Hostalot*. Aletheia [Электронный ресурс] // Веб-сайт GitHub, Inc.: [сайт]. [2021]. https://github.com/daniellerch/aletheia
7. *Guofeng Li*, *Bingwen Feng*, *Mingjin He*, *Jian Weng*, *Wei Lu*. High-capacity coverless image steganographic scheme based on image synthesis, Signal Processing: Image Communication, 2023.
8. *Пудов Д. Ю*. Определение устойчивости бесконтейнерного метода сокрытия данных к современным методам стегоанализа. Вестник Рязанского государственного радиотехнического университета. 2023. № 83. С. 102–111.

Дата поступления рукописи
в редакцию 15.04.2024
Дата принятия рукописи
в печать 10.07.2024