## Заключение

Предложенное расширение является развитием современных подходов фаззинга виртуальных машин JavaScript. В результате удалось существенно повысить эффективность тестирования на уязвимости, расширив метод фаззинга, использующего мутации абстрактных синтаксических деревьев, и значительно увеличить скорость обнаружения новых путей исполнения в тестируемой программе. Исходный код реализованного фаззера доступен для изучения и использования на портале github [7].

ЛИТЕРАТУРА

1. Domato Fuzzer. `https://github.com/googleprojectzero/domato/blob/master/README.md`. 2021.
2. Dharma Fuzzer. `https://github.com/MozillaSecurity/dharma/blob/master/README.md`. 2021.
3. *Aschermann C.* NAUTILUS: Fishing for Deep Bugs with Grammars. `https://www.syssec.ruhr-uni-bochum.de/media/emma/veroeffentlichungen/2018/12/17/NDSS19-Nautilus.pdf`. 2021.
4. *Aho A. V., Lam M. S., Sethi R., and Ullman J. D.* Compilers: Principles, Techniques, and Tools. Addison Wesley, 2007.
5. Виртуальная машина JavaScript SpiderMonkey. `https://developer.mozilla.org/en-US/docs/Mozilla/Projects/SpiderMonkey`. 2021.
6. Виртуальная машина JavaScript ChakraCore. `https://github.com/chakra-core/ChakraCore`. 2021.
7. `https://github.com/MashaSamoylova/DFuzzer/blob/master/README.md`. 2021.

УДК 004.056 DOI 10.17223/2226308X/14/32

# РАСШИРЕНИЕ И ИССЛЕДОВАНИЕ МЕТОДА СОКРЫТИЯ ИНФОРМАЦИИ DEEP STEGANOGRAPHY

А. А. Николаев

Программно реализован метод сокрытия информации с помощью нейронных сетей Deep Steganography. Предложено и реализовано расширение метода в виде добавления дополнительных скрытых слоёв в закодированное изображение для возможности передачи большего объёма информации. Исследованы качества и свойства предложенного метода сокрытия информации.

**Ключевые слова:** *сокрытие информации, скрытые каналы, нейронные сети.*

## 1. Сокрытие информации с помощью нейронных сетей

В настоящее время известны два основных метода сокрытия информации с помощью нейронных сетей: Deep Steganography [1] и HiDDeN [2]. Основным их различием является возможный тип передаваемых данных: в случае Deep Steganography в качестве секретного сообщения выступает изображение; в случае HiDDeN — любая битовая последовательность.

В работе исследуется расширение метода сокрытия информации с помощью нейронных сетей Deep Steganography.

Метод Deep Steganography впервые описан в работе [1]. Схема сокрытия и раскрытия секретного изображения состоит из трёх нейронных сетей, которые обучаются одновременно как единая сеть, но работают независимо друг от друга и могут быть

разделены между отправителем и получателем. Данный метод позволяет скрывать секретное изображение внутри изображения-контейнера с помощью подготовительной (prep network) и скрывающей (hiding network) сетей, которые находятся на стороне отправителя, и раскрывать секретное изображение на стороне получателя с помощью раскрывающей (reveal network) сети.

## 2. Расширение метода Deep Steganography

В результате реализации метода Deep Steganography разработано и предложено расширение метода в виде добавления дополнительных скрытых слоёв в закодированное изображение.

Основной принцип работы и роль сетей аналогичны оригинальному методу Deep Steganography, за исключением того, что вместо одной подготовительной и одной раскрывающей сети используются $n$ подготовительных и $n$ раскрывающих сетей — таким образом, модифицируется архитектура самой сети. Каждая из сетей позволяет закодировать в изображении-контейнере и раскрыть $n$ изображений соответственно. Число $n$ определяется допустимым уровнем искажений в контейнере и потребностью в необходимом числе секретных изображений, которое требуется закодировать и передать — при сокрытии большего числа сообщений в виде изображений исходное изображение-контейнер подвергается большим искажениям, чем при использовании меньшего числа сообщений.

Скрывающая сеть принимает на вход одно изображение-обложку и $n$-секретных изображений. Раскрывающие сети способны раскодировать набор секретных изображений (каждая сеть раскодирует свой слой, содержащий секрет).

Данное расширение позволяет передать больший объём скрытой информации за один сеанс передачи (при использовании одного медиаконтейнера) по сравнению с классическим методом.

В качестве основной библиотеки для разработки была использована TensorFlow. Для подготовки и тренировки модели в качестве тренировочного набора данных был выбран датасет Tiny ImageNet, который является уменьшенной версией датасета ImageNet. Датасет Tiny ImageNet содержит 200 категорий изображений, по 500 изображений размера $64 \times 64$ пикселя в каждой. Суммарно Tiny ImageNet содержит 100 000 изображений.

В качестве основной метрики оценки качества восстановления исходных изображений был выбран индекс структурного сходства (индекс SSIM, Structural Similarity Index Measure). Данный индекс позволяет определить структурную схожесть между двумя изображениями методом полного сопоставления. Значение, близкое к 1,0 (или 100 % в интерпретации), достигается только при полной аутентичности двух образцов.

Для анализа было выбрано 10 случайных наборов изображений из датасета Tiny ImageNet, каждый из которых включает в себя изображение-обложку и изображение-контейнер, а также $n$ изображений, подготовленных для сокрытия в контейнере. В экспериментах $n = 3$, что является оптимальным для сокрытия и передачи данных. Проведён полный процесс сокрытия и раскрытия изображений в каждом из наборов, данные представлены в таблице, где $I_0$ — индекс схожести обложки и контейнера; $I_k$ — индекс схожести секрета и восстановленного изображения для слоя $k$, $k = 1, 2, 3$; наивысшее значение индекса выделено полужирным шрифтом.

Таким образом, предложенное расширение позволяет восстановить секретное изображение в среднем с точностью 82 % для ближайшего к обложке слоя изображения (третьего) и 56 % для наиболее глубоко скрытого слоя (первого).

| № п/п | $I_0$, % | $I_1$, % | $I_2$, % | $I_3$, % |
|---|---|---|---|---|
| 1 | 70 | 56 | 81 | 81 |
| 2 | 70 | **71** | 71 | 76 |
| 3 | 59 | 55 | **85** | **88** |
| 4 | 58 | 49 | 80 | 85 |
| 5 | 64 | 45 | 68 | 80 |
| 6 | **78** | 49 | 72 | 86 |
| 7 | 72 | 63 | 75 | 82 |
| 8 | 63 | 52 | 68 | 81 |
| 9 | 74 | 68 | 83 | 82 |
| 10 | 63 | 54 | 82 | 85 |
| **Среднее** | 67 | 56 | 76 | 82 |

Для оценки качества сокрытия данных в контейнере использован также программный инструмент StegSolve, позволяющий обнаружить артефакты и скрытую информацию в медиаконтейнерах. В результате анализа изображения-контейнера с помощью StegSolve восстановить скрытые изображения или обнаружить артефакты без раскрывающей сети не удалось, что свидетельствует о том, что данный метод имеет высокую надёжность передачи сообщений без возможности восстановления скрытых изображений участником, не имеющим доступа к раскрывающей сети.

## ЛИТЕРАТУРА

1. *Baluja S.* Hiding Images in Plain Sight: Deep Steganography // Adv. Neural Inform. Processing Systems. 2017. No. 30. P. 1–11.
2. *Zhu J., Kaplan R., Johnson J., and Fei-Fei L.* HiDDeN: Hiding Data With Deep Networks. 2018. `https://arxiv.org/abs/1807.09937`.

УДК 519.23:519.6: 004.052 DOI 10.17223/2226308X/14/33

# АДАПТАЦИЯ МЕТОДА РОЗЕНБЛАТТА — ПАРЗЕНА ДЛЯ ЭКСПЕРИМЕНТАЛЬНОЙ ОЦЕНКИ НАДЁЖНОСТИ ВЫЧИСЛИТЕЛЬНОЙ СИСТЕМЫ

В. С. Никулин

Отсутствие исходной информации о законе распределения случайных величин и их реализация в момент, близкий к началу наблюдения, а также наличие цензурированных данных вызывает необходимость адаптации непараметрического метода Розенблатта — Парзена. Для компенсации смещения и устранения нарушения условия нормировки рассмотрен метод зеркального отображения исходных данных. При построении плотности распределения случайных величин предлагается учитывать цензурированные данные. Проведённая оценка точности показывает уменьшение ошибки при аппроксимации эмпирической плотности распределения адаптированным методом Розенблатта — Парзена. На примере экспериментальной оценки показателей надёжности вычислительной системы продемонстрирована практическая реализация адаптированного метода Розенблатта — Парзена. Построение плотности и функции распределения времени до отказа позволяет рассчитать основные показатели безотказности объекта: интенсивность отказов, вероятность безотказной работы, среднее время наработки на отказ.

**Ключевые слова:** *экспериментальный анализ надёжности, малые выборки, вычислительные системы, метод Розенблатта — Парзена.*