УДК 004.931
ББК 32.813.52
Ч 25

Частикова В.А.
Кубанский государственный технологический университет, Краснодар, Россия, chastikova_va@mail.ru
Аббасова С.С.
Кубанский государственный технологический университет, Краснодар, Россия, svetlana.pet97@mail.ru

Аспекты применения сверточных нейронных сетей при обнаружении скрытой информации в изображениях

(Рецензирована)

Аннотация. *Рассматривается подход к решению проблем стегоанализа с использованием механизмов искусственных нейронных сетей. Описана концепция методики стеганографического анализа изображений, которая состоит в синтезе сигнатурного и статистического алгоритмов, а также сверточных нейронных сетей. Роль сигнатурного метода заключается в проверке наличия возможных пустых контейнеров в изображении и их наполненности. При положительном отклике изображение сканируется методом хи-квадрат. Применение искусственных нейронных сетей позволяет повысить надежность обнаружения скрытых сообщений в цифровых файлах и чувствительность к стеговложениям. Описаны механизмы работы предложенной методики, приводится обоснование выбора архитектуры сверточной нейронной сети. Обученная нейросеть может фиксировать сложные зависимости, которые используются при анализе изображения на наличие скрытой информации и более точно обнаруживать стеговложения посредством применения сверточных слоев. К преимуществам предложенного подхода можно отнести снижение временных затрат и упрощение поиска сокрытой информации.*

Ключевые слова: *стегоанализ, защита информации, цифровое изображение, сигнатурный метод, метод хи-квадрат, искусственные нейронные сети, сверточные нейронные сети*

Chastikova V.A.
Kuban State University of Technology, Krasnodar, Russia, chastikova_va@mail.ru
Abbasova S.S.
Kuban State University of Technology, Krasnodar, Russia, svetlana.pet97@mail.ru

Aspects of using convolutional neural networks for detecting hidden information in images

Abstract*. This study presents an approach to solving the problems of steganalysis using the mechanisms of artificial neural networks. The paper describes the concept of steganographic image analysis technique, which consists in the synthesis of signature and statistical algorithms, as well as convolutional neural networks. The role of the signature method is related to checking empty containers in their filling. If the response is positive, the image is scanned using the chi-square method. The use of artificial neural networks makes it possible to increase the reliability of detecting hidden messages in digital files and sensitivity to staggering. The article describes the mechanisms of the proposed methodology and the rationale for the choice of the architecture of the convolutional neural network. A trained neural network can capture complex dependencies used with image analysis for hidden information, and more accurately detect steg-nesting using convolutional layers. The advantages of the proposed approach include a reduction in time costs and a simplified search for hidden information.*

Keywords*: steganalysis, information protection, digital image, signature method, chi-square method, artificial neural networks, convolutional neural networks*

Введение

Вопросы информационной безопасности будут актуальными всегда. Необходимость защиты информации обусловлена ростом компьютерной преступности, поэтому в настоящее время уделяется большое внимание предотвращению утечек и кражи секретных данных [1]. Существует множество способов несанкционированного получения защищаемой информации, к одному из них можно отнести методы стеганографии. Ежедневно в сети Интернет достаточно большое количество людей обмениваются файлами, не подозревая о возможном секретном содержимом в них. Одним из наиболее распространенных стеганографических контейнеров является цифровое изображение [2]. При встраивании сообщения человеческому глазу сложно распознать малейшие изменения в изображении. Проблему использования стеганографии помогают решить методы стегоанализа. Их основная цель – обнаружить наличие секретного сообщения в цифровом изображении. Обычно эта задача формулируется как проблема бинарной классификации, позволяющая различать содержащие и не содержащие стеговложения изображения. В этом случае существующие методы стегоанализа создаются в два этапа: извлечение признаков и классификация. На этапе извлечения признаков используется набор созданных вручную функций, полученный из каждого изображения, чтобы понять влияние операций встраивания. Однако отсутствие точных моделей естественных изображений усложняет эту работу [3].

Основные принципы используемого подхода стеганографического анализа изображений на основе сигнатурного и статистических методов

Алгоритм работы предложенной ранее методики (представлен на рисунке 1) заключается в последовательном применении сигнатурной и статистической атак для возможности обработки большего количества данных. При попадании изображения в поток данных оно предварительно сканируется сигнатурным методом. Данный метод проверяет наличие возможных пустых контейнеров в изображении и их наполненность. Как правило, не все изображения имеют свободные контейнеры в палитре RGB или же объем этих контейнеров очень мал, что позволяет судить о том, что в данном файле нет зашифрованной информации. Если же сигнатурный метод опознает наличие контейнера или его заполненность, то далее файл анализирует уже статистический метод хи-квадрат. Делается это для того, чтобы максимально сэкономить время обработки файлов в потоке данных и большей надежности [4].

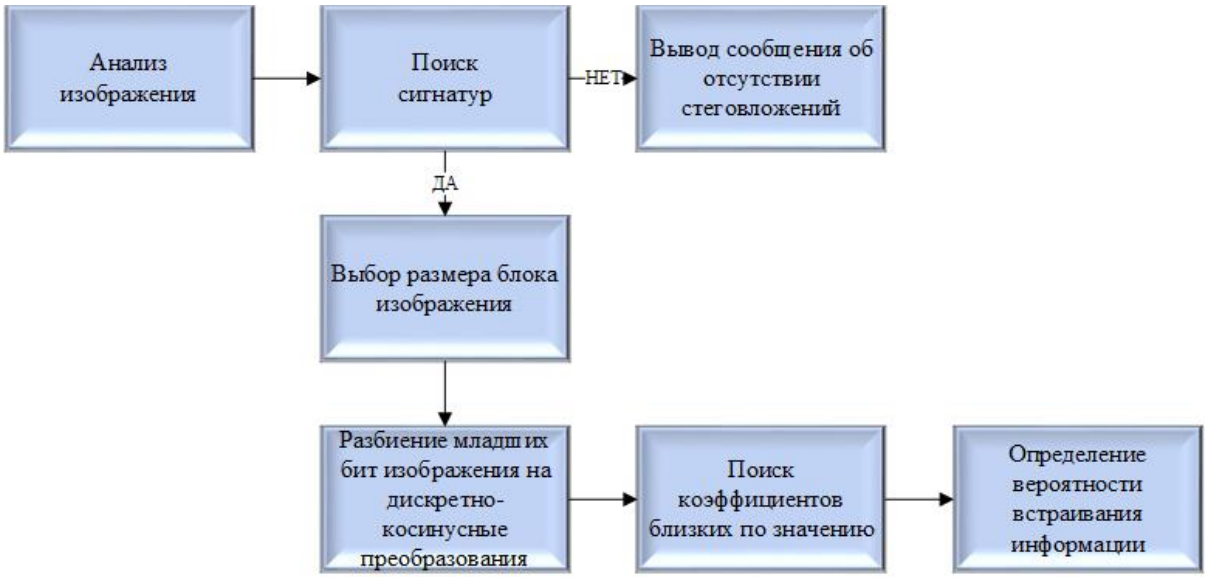

Рис. 1. Методика стегоанализа цифровых изображений

Подключение атаки хи-квадрат при обнаружении контейнера или его заполненности обязательно, так как сигнатурный метод недостаточно надежен и не может дать полную оценку, возможно только провести предварительный анализ. Стеганографические вложения изменяют гистограмму косинусных коэффициентов, что сразу заметно программе.

Метод хи-квадрат является универсальным, так как подходит для анализа изображений, созданных различными программами скрытия, что делает предложенную методику обнаружения скрытой информации более стойкой и актуальной.

В последнее время ряд исследований в области стегоанализа, в частности цифровых изображений, посвящен применению методов машинного обучения, основанных на использовании искусственных нейронных сетей. Поскольку при стегоанализе используются трудоемкие в реализации численные методы, применение нейронных сетей снизит временные затраты и упростит алгоритм обнаружения стеговложений.

С использованием таких подходов решается задача бинарной классификации цифровых изображений – разделения их множества на подмножества, содержащие и не содержащие стеговложения [5].

Описание методики применения сверточных нейронных сетей в стегоанализе цифровых изображений

Задачи стегоанализа сильно отличаются от задач искусственных нейронных сетей. След стеганографического внедрения сообщения в цифровое изображение сложно распознать системе восприятия человека, следовательно, достаточно трудно обучить этому нейронную сеть. Однако если уменьшить количество параметров поиска стеговложений в изображениях и улучшить качество распознавания признаков, то обучение будет реализовано быстрее и удастся оптимизировать сложность вычислительных процессов, как, например, при распознавании паттернов нейронной сетью Хопфилда [6].

В предлагаемом подходе используются сверточные нейронные сети. Их применение дает возможность обнаружить определенные характеристики не в целом изображении, а в его частях. Такая особенность достигается сегментацией изображения во время прохождения ядра сверточной нейронной сети (СНС). Как правило, СНС делится на несколько слоев, а именно: на сверточные, слои подвыборки или слои обработки изображений и полносвязные [7].

Одним из важнейших этапов алгоритмов стегоанализа, основанных на использовании нейросетевого аппарата, является выбор признаков, по которым нейронная сеть будет делать вывод о наличии стеговложений. Пространство пикселей изображения превращается в пространство признаков, и определение наличия встроенного сообщения происходит уже в нем.

В стегонализе считается, что для цифровых изображений последующая обработка в камере во время получения изображения (интерполяция цвета, шумоподавление, цветокоррекция и фильтрация) вносит сложные зависимости в шумовую составляющую соседних пикселей. Но стегошум нарушит эти зависимости. Большинство методов стегонализа пытаются использовать подобные зависимости для обнаружения присутствия стегошума [8]. Эвристически предполагается, что из-за сложных зависимостей хорошую оценку центрального пикселя можно получить из соседних пикселей, за исключением оцениваемого пикселя. Путем вычитания истинного значения центрального пикселя из оценочного значение ошибки обнаружения можно определить, был ли пиксель изменен.

На рисунке 2 представлена схема методики использования сверточной нейронной сети для стегоанализа цифровых изображений.

Суть предложенной методики заключается в выявлении стеговложений, а также

в оценке точности классификации и отнесения изображений к определенному множеству. Наборы цифровых изображений могут быть взяты на любом открытом ресурсе.

Рис. 2. Методика применения СНС для стегоанализа изображений

Шаг применения двумерной свертки предполагает операцию уменьшения размера изображения, а именно его деление на пиксели и получение на выходе нового элемента (а именно – пикселя) последующего слоя нейронной сети. Краткое представление этого шага изображено на рисунке 3.

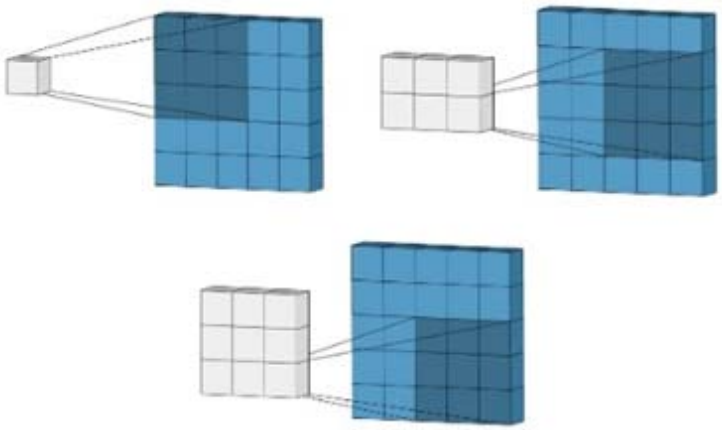

Рис. 3. Операция «Двумерная свертка»

Пулинг также позволяет уменьшить размер анализируемого изображения, но непосредственно с целью минимизации операций над ним. На последнем этапе производится классификация, то есть отнесение выявленных закономерностей к изображениям, либо содержащим стеговложения, либо не содержащим их. Использование нескольких слоев сверточной нейронной сети дает возможность более детально проанализировать цифровой файл и выявить наборы зависимостей, и впоследствии их классифицировать.

Заключение

Основной целью при разработке методики являлась оптимизация алгоритмов стегоанализа, поэтому было предложено современное решение, которое помогает уменьшить сложность математических вычислений и снижает времязатратность на них.

Обученная нейронная сеть может фиксировать сложные зависимости, которые используются в стегоанализе, и более точно обнаруживать стеговложения посредством применения сверточных слоев. По мере того, как сеть обучается и углубляется, возни-

кают более сложные зависимости, которые моделируются путем постепенной обработки больших входных данных.

Список литературы:

1. Кучер В.А., Зангиев Т.Т., Тарасов Е.С. Применение автоматизированных комплексов и учебно-тренировочных средств для изучения вопросов управления информационной безопасностью // Информационное противодействие угрозам терроризма. 2015. Т. 1, № 25. С. 240–244.
2. Вахаб А., Романенко Д.М. Методы цифровой стеганографии на основе модификации цветовых параметров изображения // Труды БГТУ. Сер. 3. 2018. № 1. С. 94–98.
3. Mehdi Yedroudj, Frederic Comby, Marc Chaumont, Yedroudj-net: An efficient CNN for spatial steganalysis, ICASSP: International Conference on Acoustics, Speech and Signal Processing, Date of Conference: 15–20 April 2018. Calgary: Alberta, 2018, Canada.
4. Частикова В.А., Аббасов Т.О., Аббасова С.С. Методика распознавания скрытой информации в изображениях на основе алгоритмов стеганографии // Вестник Адыгейского государственного университета. Сер.: Естественно-математические и технические науки. 2020. Вып. 3 (266). С. 40–45. URL: http://vestnik.adygnet.ru
5. Deep learning for steganalysis via convolutional neural networks / Y. Qian, J. Dong, W. Wang, T. Tan // Proceedings SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics, February 8–12, 2015 / A. Alattar, N.D. Memon, editors. San Francisco, 2015. Vol. 9409. P. 1–10.
6. Частиков А.П., Малыхина М.П., Урвачев П.М. Анализ распознавания паттернов нейросетевыми методами // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2014. № 98. С. 457–467. URL: http://ej.kubagro.ru/2014/04/pdf/43.pdf
7. Частикова В.А., Жерлицын С.А., Воля Я.И. Нейросетевой подход к решению задачи построения фоторобота по словесному описанию // Известия Волгоградского государственного технического университета. 2018. № 8 (218). С. 63–67.
8. Mehdi Boroumand, Mo Chen, Jessica Fridrich. Deep Residual Network for Steganalysis of Digital Images // IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, Iss. 5. P. 1181–1193.

References:

1. Kucher V.A., Zangiev T.T., Tarasov E.S. The use of automated complexes and training tools for studying the issues of information security management // Information Counteraction to the Threats of Terrorism. 2015. Vol. 1, No. 25. P. 240–244.
2. Vakhab A., Romanenko D.M. Methods of digital steganography based on the modification of color parameters of the image // Proceedings of BSTU. Ser. 3. 2018. No. 1. P. 94–98.
3. Mehdi Yedroudj, Frederic Comby, Marc Chaumont, Yedroudj-net: An efficient CNN for spatial steganalysis, ICASSP: International Conference on Acoustics, Speech and Signal Processing, Date of Conference: 15–20 April 2018. Calgary: Alberta, 2018, Canada.
4. Chastikova V.A., Abbasov T.O., Abbasova S.S. Methods for recognizing hidden information in images based on steganography algorithms // The Bulletin of the Adyghe State University. Ser.: Natural-Mathematical and Technical Sciences. 2020. Iss. 3 (266). P. 40–45. URL: http://vestnik.adygnet.ru
5. Deep learning for steganalysis via convolutional neural networks / Y. Qian, J. Dong, W. Wang, T. Tan // Proceedings SPIE, Electronic Imaging, Media Watermarking, Security, and Forensics, February 8–12, 2015 / A. Alattar, N.D. Memon, editors. San Francisco, 2015. Vol. 9409. P. 1–10.
6. Chastikov A.P., Malykhina M.P., Urvachev P.M. Analysis of pattern recognition by neural network methods // Polythematic Network Electronic Scientific Journal of the Kuban State Agrarian University. 2014. No. 98. P. 457–467. URL: http://ej.kubagro.ru/2014/04/pdf/43.pdf
7. Chastikova V.A., Zherlitsyn S.A., Volya Ya.I. Neuronetwork approach to the solution of the problem of construction of an identikit using a verbal description // News of Volgograd State Technical University. 2018. No. 8 (218). P. 63–67.
8. Mehdi Boroumand, Mo Chen, Jessica Fridrich. Deep Residual Network for Steganalysis of Digital Images // IEEE Transactions on Information Forensics and Security. 2019. Vol. 14, Iss. 5. P. 1181–1193.