DOI 10.37882/2223–2966.2021.08.15

НЕЙРОСЕТЕВЫЕ ТЕХНОЛОГИИ — ОСНОВНЫЕ ТРЕНДЫ РАЗВИТИЯ В УСЛОВИЯХ ГЛОБАЛЬНОЙ ЦИФРОВИЗАЦИИ

NEURAL NETWORK TECHNOLOGIES — THE MAIN DEVELOPMENT TRENDS IN THE CONTEXT OF GLOBAL DIGITALIZATION

E. Cozac

Summary. Global digitalization is associated with the widespread introduction of artificial intelligence technologies based on artificial neural networks. Such networks reflect the behavior of the human brain, allowing computer programs to recognize patterns and solve various problems from image recognition to the search for diseases.

Neural networks are based on specially configured learning algorithms for specific tasks that allow classifying and clustering disparate data at a high speed, which allows neural networks to recognize speech, text or images in minutes. However, despite the already known advantages of neural networks, various studies are currently continuing, aimed both at optimizing the learning processes of neural networks, and at choosing the best neural network structure in accordance with the features and complexities of the problem proposed for a system equipped with artificial intelligence.

One of these research areas is the development of convolutional neural networks used for the purposes of computer vision technologies. The above-mentioned networks are able to create music and paintings, detect diseases and solve many other tasks that were previously considered exclusively anthropic — solvable only by humans. However, despite all the advantages of such networks, their possibilities are not unlimited, in addition, convolutional neural networks are quite vulnerable to various kinds of attacks, so research in the field of convolutional networks continues, and the topic of the development of such networks is one of the most relevant in the field of neural network technologies.

Keywords: neural networks, global digitalization, neural network technologies, convolutional neural networks, vulnerability of neural networks.

Козак Евгений
Старший разработчик, Memery Crystal LLP, Лондон, Англия
eugeniu.cozac@gmail.com

Аннотация. Глобальная цифровизация связана с повсеместным внедрением технологий искусственного интеллекта, основанного на искусственных нейронных сетях. Такие сети отражают поведение мозга человека, позволяя компьютерным программам распознавать закономерности и решать различные проблемы, начиная от распознавания изображений и заканчивая поиском болезней.

В основе работы нейронных сетей лежат специально настроенные на конкретные задачи алгоритмы обучения, которые могут классифицировать и кластеризировать разрозненные данные с высокой скоростью, что позволяет нейронным сетям распознавать речь, текст или изображений за минуты. Однако несмотря на уже известные преимущества нейронных сетей, в настоящий момент продолжаются различные исследования, направленные как на оптимизацию процессов обучений нейронных сетей, так и на выбор наилучшей структуры нейронной сети в соответствии с особенностями и сложностями задачи, предлагаемой к решению для системы, снабженной искусственным интеллектом.

Одним из таких исследовательских направлений является развитие свёрточных нейронных сетей, используемых для целей технологий компьютерного зрения. Вышеназванные сети способны создавать музыку и картины, выявлять болезни и решать многие другие задачи, которые раньше считались исключительно антропными, то есть разрешимыми только человеком. Тем не менее, несмотря на все преимущества таких сетей, возможности их не безграничны, кроме того, свёрточные нейронные сети достаточно уязвимы перед различного рода атаками, поэтому исследования в данной области продолжаются, а тематика развития таких сетей является одной из самых актуальных в области нейросетевых технологий.

Ключевые слова: нейронные сети, глобальная цифровизация, нейросетевые технологии, сверточные нейронные сети, уязвимость нейронных сетей.

Сегодня нейронные сети составляют основу, посредством которой обеспечивается функционирование искусственного интеллекта, без которого в условиях глобальной цифровизации не обходится ни один цифровой процесс. Однако, несмотря на то, что первые концепции искусственных нейронных сетей были предложены в конце 90-х годов XIX века [1, 2, 3], а в настоящий момент наблюдается их глобальное использование, до сих пор продолжаются исследования, направленные как на изучение особенностей работы таких сетей в различных цифровых технологиях, так и на совершенствование работы нейронных сетей, в том числе за счет оптимизации процессов их обучения.

Такой практический интерес к развитию искусственных нейронный сетей обусловлен их особенностями и значением для целей различных технологий в бизнесе, медицине, технике, геологии, физике, военной деятельности и пр. Так, например, нейронные сети могут помочь понять взаимосвязи между сложными структурами данных. Нейронные сети могут использовать полученные знания для прогнозирования поведения сложных структур. Нейронные сети могут быть использованы для прогнозирования линейных и нелинейных взаимосвязей в данных, а также обрабатывать изображения и даже принимать сложные решения, например, о том, как управлять автомобилем или какую финансовую сделку выполнять дальше.

Искусственные нейронные сети в наиболее общем понимании представляют собой математические модели, построенные на определенных принципах и имеющие возможности глубокого обучения для различных задач с использованием искусственного интеллекта [3]. В основе таких определенных принципов лежит организация и функционирование сетей нервных клеток (нейронов) человеческого мозга (их биологических аналогов). Исходя из сказанного, искусственная нейронная сеть построена на идее возможности моделирования нейронов с помощью простых автоматов (искусственных нейронов), поскольку вся сложность человеческого мозга объясняется связями между нейронами [5, 8, 9].

Сама по себе функция активации нейронной сети представляет собой математическую формулу, которая помогает нейрону включаться или выключаться. Особенности же активации нейронной сети зависят от структуры нейронной сети, потока данных, используемых нейронов и их плотности, слоев и глубинных фильтров активации. В специализированной литературе и на практике принято выделять множество нейронных сетей — многослойный персептрон, сети обратной связи, персептрон, модульные сети, рекуррентные сети, сети радиальной базисной функции, сверточные сети и пр. Выбор структуры нейронной сети осуществляется в соответствии с особенностями и сложностями задачи, предлагаемой к решению для системы, снабженной искусственным интеллектом.

Например, безусловными преимуществами многослойных нейронных сетей являются возможности их глубокого обучения за счет наличия плотных полностью связанных слоев и возможностей обратного распространения, а недостатками таких сетей являются сложности в их проектировании и обслуживании. Однако наибольший научный интерес начиная с 2012 года прикован к другому виду нейронных сетей — сверточным нейронным сетям, которые называют «самой важной инновацией в области компьютерного зрения» [6, 7].

Впервые о преимуществах сверточных нейронных сетей стало известно в 2012 году, когда Алекс Крижевски использовал такие сети для победы в конкурсе ImageNet (ежегодные Олимпийские игры по компьютерному зрению), снизив за счет использования сверточной сети показатель ошибок с 26% до 15%. Однако разработаны сверточные нейронные сети, также называемые ConvNets, были еще в 1980-х годах Яном Лекуном. Ранняя версия сверточных нейронных сетей, получившая название LeNet (в честь Я. Лекуна), могла распознавать рукописные цифры.

Вместе с тем, несмотря на все свои преимущества, сверточные нейронные сети долгое время оставались в стороне от компьютерного зрения и искусственного интеллекта, потому что их использование было сопряжено с проблемой, которую нельзя было решить в конце 80-х годов прошлого века — такие сети не могли масштабироваться, при этом требовалось много данных и вычислительных ресурсов для эффективной работы с большими изображениями, а все достижения техники того времени были применимы только к изображениям с низким разрешением.

Главной особенностью сверточной нейронной сети является то, что она содержит трехмерное расположение нейронов вместо стандартного двумерного массива. Первый слой называется сверточным. Каждый нейрон в сверточном слое обрабатывает информацию только из небольшой части поля зрения. Входные характеристики берутся пакетно, как фильтр. Сеть понимает изображения по частям и может вычислять эти операции несколько раз, чтобы завершить полную обработку изображений. Обработка включает в себя преобразование изображения из RGB или HSI масштаба в серый масштаб. Дальнейшее изменение значения пикселя поможет обнаружить края, и изображения могут быть классифицированы по разным категориям. Фильтры в сверточных слоях модифицируются на основе изученных параметров для извлечения наиболее полезной информации для конкретной задачи. Сверточные сети автоматически настраиваются для поиска наилучшей функции в зависимости от поставленной задачи. Сверточная сеть, как и любая другая нейронная сеть, будет фильтровать информацию о форме объекта, когда столкнется с общей задачей распознавания объектов, но будет извлекать конкретные данные, когда будет направлена на конкретную задачу.

Распространение является однонаправленным, когда сверточная сеть содержит один или несколько сверточных слоев, за которыми следует объединение, и двунаправленным, когда выходной сигнал сверточного слоя поступает в полностью связанную нейронную сеть для классификации изображений. Фильтры

используются для извлечения определенных частей изображения. Именно поэтому сверточные нейронные сети показывают очень эффективные результаты в распознавании изображений и видео, семантическом анализе и обнаружении парафраз в текстовых документах.

При решении задачи классификации изображений с использованием искусственных нейронных сетей число обучаемых параметров резко возрастает с увеличением размера изображения. Сверточные нейронные сети фиксируют пространственные особенности изображения, чего не могут сделать любые другие нейронные сети. Именно поэтому сверточные нейронные сети стали основным методом для решения любой задачи с данными изображений. Все популярные фреймворки поддерживают сверточные нейронные сети, такие, как Tensorflow-Keras и PyTorch.

После обучения сверточной нейронной сети разработчики используют тестовый набор данных для проверки его точности. Тестовый набор данных — это набор помеченных изображений, которые не являются частью процесса обучения. Каждое изображение проходит через сверточную нейронную сеть, и выход сравнивается с фактической меткой изображения. По сути, тестовый набор данных оценивает, насколько хорошо нейронная сеть научилась классифицировать изображения, которых она раньше не видела.

Однако, несмотря на то, что сверточные нейронные сети являются мощными моделями, при их реализации все же могут возникнуть некоторые проблемы, среди которых — необходимость использования большого объёма вычислительной мощности, необходимость в большом объеме данных для обучения, трудность в интерпретации отдельных данных ввиду того, что обучение нейронных сетей все еще является развивающейся и быстро меняющейся областью.

Несмотря на свою мощность и сложность, сверточные нейронные сети по свой сути являются машинами распознавания образов. Они могут использовать огромные вычислительные ресурсы, чтобы выискивать крошечные и незаметные визуальные паттерны, которые могут остаться незамеченными для человеческого глаза. Но когда дело доходит до понимания смысла содержания образов, они работают плохо.

Эти ограничения становятся более очевидными в практических приложениях сверточных нейронных сетей. Например, сверточные нейронные сети сейчас широко используется для модерирования контента в социальных сетях. Но, несмотря на обширные хранилища изображений и видео, на которых они обучены, сверточные нейронные сети пытаются обнаружить и заблокировать неподходящий контент. Примечательным является случай, когда сверточные нейронные сети Facebook по модерации контента запретили использование фотографии статуи 30000-летней давности, отметив ее как потенциально неприемлемое изображение обнаженного тела.

Кроме того, нейронные сети начинают ломаться, как только они немного выходят из своего контекста. Несколько исследований показали, что сверточные нейронные сети, обученные на ImageNet и других популярных наборах данных, не могут обнаружить объекты, когда они видят их при различных условиях освещения и под новыми углами.

Другой проблемой сверточных нейронных сетей является их неспособность понять отношения между различными объектами, что отчетливо прослеживается при решении «проблемы Бонгарда», названной в честь его изобретателя, русского ученого в области информационных технологий Михаила Моисеевича Бонгарда.

Решение «проблемы Бонгарда» заключается в представлении для выбора двух наборов изображений (шесть слева и шесть справа), и необходимости объяснить ключевое различие между этими двумя наборами. Людям легко сделать соответствующие выводы из такого небольшого количества образцов. Но до сих пор нет сверточной нейронной сети, которая могла бы решить «проблемы Бонгарда» даже небольшим количеством обучающих примеров. В одном исследовании, проведенном в 2016 году, исследователи искусственного интеллекта обучили сверточную нейронную сеть на 20 000 образцах Бонгарда и протестировали его еще на 10 000. Производительность сверточной нейронной сети была намного ниже, чем у обычных людей.

Особенности сверточной нейронной сети делают их уязвимыми для различного рода атак, так как именно сверточные нейронные сети стали неотъемлемым компонентом многих важных приложений, таких, как самоуправляемые автомобили [4, 8, 10]. Поэтому в настоящий момент исследования, направленные на разработку механизмов предотвращения сбоев в работе сверточных нейронных сетей, еще только начинают развиваться [7, 10].

Подводя итог, необходимо отметить, что с каждым днем информационные технологии все глубже проникают в нашу жизнь. Так, микропроцессоры, которые вызвали технологическую революцию в 70-х годах, изменив все аспекты нашей жизни, связанные с вычислениями, теперь кажутся чем-то устаревшим, поскольку сверточные нейронные сети, используемые в компьютерах, способны создавать музыку и картины, выяв-

лять болезни и решать многие другие задачи, которые раньше считались исключительно антропными — разрешимыми только человечеством. Поэтому значимость сверточных нейронных сетей нельзя отрицать — они вызвали революцию в искусственном интеллекте. Однако, несмотря на все преимущества таких сетей, возможности их не безграничны, кроме того, сверточные нейронные сети достаточно уязвимы перед различного рода атаками, поэтому исследования в области сверточных сетей продолжаются, а тематика развития таких сетей является одной из самых актуальных в области нейросетевых технологий.

ЛИТЕРАТУРА

1. Барский А.Б. Введение в нейронные сети / Барский А.Б. — Электрон. текстовые данные. — М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 358 с.
2. Бова В.В., Дуккардт А.Н. Пприменение искусственных нейронных сетей для коллективного решения интеллектуальных задач. Известия ЮФУ. Технические науки. Хайкин С. Нейронные сети: Пер. с англ. — М.: Издательский дом «Вильямс», 2006.
3. Брагин Александр Дмитриевич, Спицын Владимир Григорьевич Распознавание моторных образов на электроэнцефалограммах с применением свёрточных нейронных сетей // КО. — 2020. — № 3. — С. 482–489.
4. Полунин А.А., Яндашевская Э.А. Использование аппарата свёрточных нейронных сетей для стегоанализа цифровых изображений // Труды ИСП РАН. — 2020. — № 4. — С. 155–164.
5. Редько, В.Г. Эволюция, нейронные сети, интеллект: Модели и концепции эволюционной кибернетики / В.Г. Редько. — М.: Ленанд, 2019. — 224 с.
6. Рутковская Д. Нейронные сети, генетические алгоритмы и нечеткие системы / Рутковская Д., Пилиньский М., Рутковский Л. — Электрон. текстовые данные. — М.: Горячая линия — Телеком, 2013. — 384 с.
7. Сикорский О.С. Обзор свёрточных нейронных сетей для задачи классификации изображений // Новые информационные технологии в автоматизированных системах. — 2017. — № 20. — С. 37–42.
8. Сысоев Д.В. Введение в теорию искусственного интеллекта: учебное пособие / Сысоев Д.В., Курипта О.В., Проскурин Д.К. — Электрон. текстовые данные. — Воронеж: Воронежский государственный архитектурно-строительный университет, ЭБС АСВ, 2014. — 171 с.
9. Rue, H.; Held, L.: Gaussian Markov Random Fields: Theory and Applications, CRC Press, Boca Raton, FL, 2005.
10. Jonas Teuwena, Nikita Moriakov, Convolutional neural networks. Handbook of Medical Image Computing and Computer Assisted Intervention. The Elsevier and MICCAI Society Book Series. 2020, p. 481–501.

Журнал «Современная наука: актуальные проблемы теории и практики»