Analytics. Использование BIG DATA для оптимизации бизнеса и информационных технологий (2017): сборник материалов между-нар. науч.-прак. конф/ редкол.: М.П. Батура [и др.]. - Минск: БГУИР, 2017. - 350 с. ISBN 978-985- 534-323- 2. - С. 177-180.

КЛАССИФИКАЦИЯ СОСТОЯНИЙ РАСТЕНИЙ С ПОМОЩЬЮ СВЁРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Барковский А.В.

Жвакина А.В. – к.т.н., доцент

Задачи, связанные с восприятием изображений и видео, называемые задачами компьютерного зрения, являются одними из самых актуальных среди задач машинного обучения. Одним из способов решения подобных задач является использование свёрточных нейронных сетей. В докладе рассматривается возможность использования свёрточных нейронных сетей для классификации растений в биологических исследованиях.

Автоматическая обработка изображений при помощи нейронных сетей может использоваться для классификации растений по виду или состоянию здоровья, обнаружения болезней, паразитов или сорных растений, автоматического отслеживания прогресса роста растения под воздействием различных факторов и многих других задач.

Задача является актуальной, так как сейчас на биологическом факультете Белорусского Государственного Университета данные мероприятия проводятся вручную, требуют больших затрат времени и человеческих ресурсов. Использование нейронной сети, способной самостоятельно отличать здоровые растения от умирающих, позволит автоматизировать процесс проведения биологических исследований. Это увеличит объём исследований, проводимых биологами, упростит наблюдение за экземплярами растений и снизит нагрузку на работников лабораторий.

Сравнительный анализ возможностей таких методов анализа изображений, как вручную подобранные свёртки[1], гистограммы цветов или ориентированных градиентов, а также самих свёрточных нейронных сетей показал, что нейронные сети наиболее эффективны для решения задачи классификации растений по состоянию. Они позволяют достичь необходимого уровня точности и обеспечивают скорость распознавания, позволяющую в некоторых условиях их использование в реальном времени.

Стоит отметить, что хотя нейронные сети-это относительно ресурсоёмкий метод обработки изображений, с развитием вычислительных компонентов (в частности, графических ускорителей) в последние годы даже они зачастую пригодны для использования в условиях ограниченных вычислительных ресурсов. К примеру, уже существует нейронная сеть, способная с высокой точностью разделять изображение на объекты, работающая со скоростью около 100 кадров в секунду даже на мобильном телефоне [2].

Также исследовался другой вид свёрточных сетей, особенно хорошо адаптированный под мобильные устройства[3]. Так как доступные в телефонах и стационарных компьютерах ресурсы продолжат расти, ресурсоёмкость нейронных сетей будет отходить на второй план, то в ближайшем будущем применимость и актуальность свёрточных сетей возрастет, особенно в рамках решаемой задачи.

Для разработки нейронной сети использована архитектура MobileNet. Среди её преимуществ:

- Низкая требовательность к ресурсам, что допускает возможность её использования в мобильных и других устройствах с низкой вычислительной мощностью.
- Уменьшенное время, необходимое на обучение сети.
- Адаптируемость под различные требования при помощи двух простых и хорошо изученных гиперпараметров.
- Относительная (в сравнении с некоторыми другими нейронными сетями) простота и небольшое количество параметров снижают тенденцию сети к переобучению, когда точность, достигнутая на тренировочных данных, не обобщается на другие входные данные.
- Точность, очень приближенная к другим намного более сложным видам свёрточных нейронных сетей.

Недостатком является то, что свёртки, разделяемые по глубине, несмотря на их эффективность, несколько снижают её точность. Также недостаточно изучена квантизация и в дальнейшей работе планируется исследовать возможность квантизации MobileNet, в частности её производительность и точность после этой процедуры.

В ходе разработки нейронной сети исследовались различные методы [4][5], позволяющие улучшить точность результатов нейронных сетей или достичь более быстрой сходимости при обучении.

При реализации модели на основе MobileNet использованы библиотеки TensorFlow и Keras, облегчающие описание, обучение и эксплуатацию нейронных сетей. Эти библиотеки появились относительно недавно и в них ещё присутствуют пробелы в обычно требуемом функционале. Поэтому были разработаны собственные компоненты для реализации необходимых возможностей.

Таким образом, нейронная свёрточная сеть, разработанная с использованием архитектуры MobileNet, облегчает задачу исследования состояния растений по внешним признакам, позволит выполнять широкомасштабные эксперименты и экономить при этом человеческие ресурсы и время.

Списокиспользованныхисточников:
1. An Introduction to different Types of Convolutions in Deep Learning. [Электронный ресурс] – Режим доступа: https://towardsdatascience.com/types-of-convolutions-in-deep-learning-717013397f4d. – Дата доступа : 12.03.2017.
2. Mobile Real-time Video Segmentation. [Электронный ресурс] – Режим доступа: https://research.googleblog.com/2018/03/mobile-real-time-video-segmentation.html. – Дата доступа: 12.03.2017.
3. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. [Электронный ресурс] – Режим доступа: https://arxiv.org/abs/1704.04861. – Дата доступа: 09.03.2017.
4. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. [Электронный ресурс] – Режим доступа: https://arxiv.org/abs/1502.03167. – Дата доступа: 12.03.2017.
5. The Marginal Value of Adaptive Gradient Methods in Machine Learning. [Электронный ресурс] – Режим доступа: https://arxiv.org/abs/1705.08292. – Дата доступа: 09.03.2017.

МЕССЕНДЖЕР С ВАРИАТИВНОСТЬЮ ИСПОЛЬЗОВАНИЯ КРИПТОСИСТЕМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Матюшонак А.Д., Валетко А.Н., Ковалёва Н.В., Ширяев Т.С.
Стройникова Е. Д. – ассистент кафедры информатики

В современном мире большинство информации передаётся через интернет, где её без особого труда можно перехватить, в связи с этим всё больше развиваются и способы её защиты. Самым простым и популярным из них является внедрение различных криптосистем.

Криптосистема – это комплексная модель, состоящая из алгоритмов шифрования и дешифрования, текстов различного объёма и содержания.

В зависимости от типа использованных алгоритмов криптосистемы соответственно делятся на симметричные, асимметричные и смешанные, в которых используются алгоритмы обоих типов. Так, при использовании симметричных криптосистем сообщение шифруется и дешифруется одним ключом, поэтому собеседникам нужно заранее договориться об используемом ключе. В асимметричных криптосистемах используются закрытый и открытый ключи. Открытый ключ пересылается от получателя к отправителю, который с помощью открытого ключа зашифрует сообщение, а получатель дешифрует сообщение с помощью закрытого ключа, который известен лишь ему.

Наибольшая производительность достигается при использовании симметричных методов шифрования, их скорость на несколько порядков выше, длина используемого ключа также заметно меньше, однако зачастую возникают трудности с безопасной передачей ключа. В связи с этим более предпочтительным является использование смешанных криптосистем. В данных криптосистемах сообщение шифруется симметричным способом, отправляется получателю, после чего асимметричным методом отправляется ключ.

Ввиду существования риска перехвата и изменения сообщения после его отправки принято использовать цифровую подпись. Для её создания необходимо вычислить хеш-функцию текста или файла, после чего полученное значение зашифровать с использованием секретного асимметричного ключа отправителя и добавить полученную строку к исходному тексту. Для того чтобы удостовериться в подлинности полученного сообщения, необходимо расшифровать хеш-функцию с использованием открытого ключа отправителя и повторно вычислить хеш-функцию исходного текста. Если обе функции совпадают, делается вывод о сохранности исходного сообщения.

С целью достаточной защиты пользовательских сообщений было разработано приложение Safend, использующее при отправке сообщений смешанную криптосистему и цифровую подпись. Пользователь может комбинировать уже имеющиеся в программе методы симметричного шифрования, произвольно выбирая для них порядок и входные данные, таким образом создавая собственный метод шифрования.

Для реализации данной цели был выбран язык программирования C#, т. к. он располагает большим количеством библиотек асимметричного шифрования, удобен в сетевом использовании для отправки и получения зашифрованных сообщений, а также является кроссплатформенным, что позволит в будущем перенести программу и на мобильные системы.

Переписка может осуществляться как между двумя пользователями, так и в групповом виде. Для переписки между двумя абонентами требуется добавить пользователя в список контактов, указав его ip и дав имя контакту, после чего его можно будет выбрать и начать переписку. Для групповой переписки необходимо, чтобы один из пользователей стал сервером, вызвав в программе соответствующую функцию, после к нему можно будет подключиться, указав его ip.

При добавлении пользователя в контакты создаётся случайный симметричный шифр, который отправляется ему по алгоритму RSA. При получении данный шифр будет сохранён как у получателя, так и у отправителя. В дальнейшем при их переписке по умолчанию будет использоваться именно это шифрование. Однако при желании пользователь может зашифровать сообщение собственным симметричным ключом, который будет отправлен по алгоритму RSA.