

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Ярославский государственный университет им. П.Г. Демидова»

Кафедра дискретного анализа

«Допустить к защите»

Заведующий кафедрой,

д.ф.-м.н., профессор

_____ Бондаренко В.А.

« 13 » июня 2020 г.

Выпускная квалификационная работа бакалавра
по направлению 01.03.02 Прикладная математика и информатика

**Анализ алгоритмов глубокого машинного обучения в задачах
распознавания изображений**

Научный руководитель

к.т.н., старший преподаватель

_____ Д.В. Матвеев

« » _____ 2020 г.

Студент группы ИВТ-41БО

_____ А.С. Коротков

« » _____ 2020 г.

Ярославль, 2020

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В настоящее время, в связи со стремительным развитием цифровых технологий, использование автоматизированных и роботизированных систем распространилось на множество областей как в промышленности, науке, так и в повседневной жизни. В следствие этого, возрастает необходимость в эффективной обработке информации, представленной, в частности, в формате видео и изображений.

На текущий момент изображения тесно влились в жизнь человека. Поэтому многие автоматизированные системы используют их в качестве основного источника информации. Нахождение, локализация, классификация и анализ образов на изображении компьютером – сложная задача компьютерного зрения.

Компьютерное (машинное) зрение – это совокупность программно-технических решений в сфере искусственного интеллекта (ИИ), нацеленных на считывание и обработку изображений, в реальном времени и без участия человека.

В настоящий момент, такие технологии применяются для решения таких сложных задач как:

- OCR – Optical character recognition (Оптическое распознавание символов): преобразование текста на изображении в редактируемый.
- Фотограмметрия – технология создания трехмерной модели объекта на основе фотографий, сделанных с различных ракурсов.
- Motion capture – технология, широко применяемая в киноиндустрии, позволяющая преобразовывать движения реальных людей в компьютерную анимацию.
- Дополненная реальность (AR) – технология, позволяющая в реальном времени проецировать виртуальные объекты на изображение реального окружения.
- Медицинская диагностика – обнаружение раковых клеток на ранней стадии, увеличение качества МРТ изображений, их анализ и т.д.

В процессе обработки информации, получаемой из глаз, человеческий мозг проделывает колоссальный объем работы. Человек без труда сможет описать что находится и что происходит на случайно взятой фотографии. Изображения могут нести в себе колоссальное количество деталей и отличаться множеством параметров, таких как: разрешение, цветность, качество, яркость, наличие шума и т.д. Объекты на изображениях также могут обладать множеством особенностей: масштаб, положение, цвет, поворот, наклон и т.д. Однако, в цифровом формате, каждое изображение представляет собой лишь массив числовых данных. Научить компьютер находить и классифицировать образы на изображении с учетом всех факторов – очень сложная алгоритмическая задача. Для её решения активно применяют технологии машинного обучения.

В данной работе был проведен анализ алгоритмов глубокого машинного обучения для решения задач распознавания изображений, а также разработана система для ЗАДАЧА.

В первой главе ...

Во второй главе ...

В третьей главе ...

csquotes
[backend=biber, sorting=nyt, bibstyle=gost-authoryear, citestyle=gost-authoryear
]biblatex

СПИСОК ИСТОЧНИКОВ

1. Michelucci U., Applied Deep Learning: A Case-Based Approach to Understanding [/ А.А. Прудникова // Мир телекома. – 2013. – №1. – С. 50-55.
2. Методические указания «Процедура системного анализа при проектировании программных систем» для студентов-дипломников дневной и заочной формы обучения специальности 7.091501 / Сост.: Сергеев Г.Г., Скاتков А.В., Машенко Е.Н. – Севастополь: Изд-во СевНТУ, 2005. – 32 с.
3. Методические указания к расчетно-графическому заданию на тему «Метод анализа иерархий» по дисциплине «Теория оптимальных решений» для студентов специальности 7.091501 «Компьютерные системы и сети» дневной и заочной формы обучения / Сост.: Ю.Н. Щепин – Севастополь: Изд-во СевНТУ, 2008. – 28 с.
4. Блюмин С.Л., Шуйкова И.А. Модели и методы принятия решений в условиях неопределенности. – Липецк: ЛЭГИ, 2001. – 138 с.
5. Hogan, M. NIST Cloud Computing Standarts Roadmap / M. Hogan, F. Liu, A. Sokol, J. Tong // NIST Special Publication 500-291, Version 2 Roadmap Working Group, 2013. – 113 с.
6. The 2016 Global Cloud Data Security Study. Ponemon Insitute LLC, 2016. – 40 с.
7. Беккер, М.Я. Информационная безопасность при облачных вычислениях: проблемы и перспективы / М.Я. Беккер, Ю.А. Гатчин, Н.С. Кармановский, А.О. Терентьев, Д.Ю. Федоров // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. – 2011. – №1(71). – С. 97-102.
8. Емельянова, Ю.Г. Анализ проблем и перспективы создания интеллектуальной системы обнаружения и предотвращения сетевых атак на облачные вычисления / Ю.Г. Емельянова, В.П. Фраленко // Программные системы: теория и приложения. – 2011. – №4(8) – С. 17-31.
9. Chisnall, D. The Definitive Guide to the Xen Hypervisor / D. Chisnall. – 1st Edition // Prentice Hall Open Source Software Development, 2007. – 320 с.
10. Федеральный закон от 21 июля 2014 г. № 242-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части уточнения порядка обработки персональных данных в информационно-телекоммуникационных сетях»

/ Минкомсвязь России // Опубликовано 12.02.2016 на официальном интернет-портале Министерства связи и массовых коммуникаций Российской Федерации

11. Облачные сервисы 2016 [Электронный ресурс] // CNews Analytics Режим доступа: <https://goo.gl/cmDSMB> (Дата обращения: 30.12.2016)
12. Cloud Security Alliance Releases 'The Treacherous Twelve' Cloud Computing Top Threats in 2016 [Электронный ресурс] // Cloud Security Alliance Research Group Режим доступа: <https://goo.gl/l2aWLu> (Дата обращения: 11.01.2017)
13. ИТ-инфраструктура предприятия 2010: Пути оптимизации [Электронный ресурс] // CNews Analytics Режим доступа: <https://goo.gl/jzrrlO> (Дата обращения: 05.01.2017)
14. Kaplan, J. Revolutionizing data center energy efficiency / J. Kaplan, W. Forrest, N. Kindler // Technical report, McKinsey & Company, 2008. – 15 с.
15. AWS signature version 1 is insecure [Электронный ресурс] // Daemonic Dispatches Режим доступа: <https://goo.gl/70bggH> (Дата обращения: 08.02.2017)
16. The CIS Critical Security Controls for Effective Cyber Defense [Электронный ресурс] // SANS website Режим доступа: <https://goo.gl/pMjbNE> (Дата обращения: 08.02.2017)
17. OWASP Top Ten Project [Электронный ресурс] // OWASP website Режим доступа: <https://goo.gl/kSHOjF> (Дата обращения: 08.02.2017)
18. CVE security vulnerability database. Security vulnerabilities, exploits, references and more [Электронный ресурс] // CVE Details. The ultimate security vulnerability datasource Режим доступа: <https://goo.gl/I3RtO2> (Дата обращения: 20.02.2017)
19. Dirty COW (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel [Электронный ресурс] // CVE-2016-5195 info website Режим доступа: <https://goo.gl/ziy3Nd> (Дата обращения: 20.02.2017)
20. Bug 1355987 - (CVE-2016-6258, xsa182) CVE-2016-6258 xsa182 xen: x86: Privilege escalation in PV guests (XSA-182) [Электронный ресурс] // Red Hat Bugzilla Режим доступа: <https://goo.gl/dlqtnR> (Дата обращения: 20.02.2017)
21. CVE-2016-5696 [Электронный ресурс] // Common Vulnerabilities and Exposures. The Standart for Information Security Vulnerability Names Режим доступа: <https://goo.gl/xYpFQQ> (Дата обращения: 21.02.2017)
22. CVE-2016-5696 [Электронный ресурс] // Debian Security Bug Tracker Режим доступа: <https://goo.gl/BXkTiL> (Дата обращения: 21.02.2017)
23. CVE-2016-8655 - Red Hat Customer Portal [Электронный ресурс] // Red Hat Customer Portal Режим доступа: <https://goo.gl/QhVbmm> (Дата обращения: 21.02.2017)

24. CVE-2016-4997 [Электронный ресурс] // Common Vulnerabilities and Exposures. The Standart for Information Security Vulnerability Names Режим доступа: <https://goo.gl/dbtXny> (Дата обращения: 21.02.2017)
25. CVE-2016-4484: Cryptsetup Initrd root Shell [Электронный ресурс] // Hector Marco Gisbert - Lecturer and Cyber Security Researcher website Режим доступа: <https://goo.gl/Jrfg6H> (Дата обращения: 22.02.2017)
26. CVE-2016-1583 [Электронный ресурс] // Debian Security Bug Tracker Режим доступа: <https://goo.gl/PIdqGR> (Дата обращения: 22.02.2017)
27. gbonacini/CVE-2016-5195: A CVE-2016-5195 exploit example. [Электронный ресурс] // GitHub Режим доступа: <https://goo.gl/9tFhHh> (Дата обращения: 24.02.2017)

СПИСОК ІЛЛЮСТРАТИВНОГО МАТЕРІАЛА

СПИСОК ТАБЛИЧНОГО МАТЕРИАЛА