Ссылка на статью:
// Ученые записки УлГУ. Сер. Математика и информационные технологии. УлГУ. Электрон. журн. 2017, № 1, с.1-4.

Поступила: 21.06.2017
Окончательный вариант: 24.09.2017

УДК 004.93'12.056.52

Применение свёрточных нейронных сетей для идентификации пользователей мобильных устройств

Анисимов А.А. [1,*]

[*] anis2005@mail.ru
[1]УлГУ, Ульяновск, Россия

Статья посвящена разработке нейросетевой системы идентификации пользователей мобильных устройств на основе данных, получаемых от использования сенсорного экрана. Произведен анализ существующих систем идентификации. Предложен метод распознавания с использованием свёрточных нейронных сетей для идентификации владельца устройства.

***Ключевые слова**: свёрточная нейронная сеть, биометрическая идентификация, мобильное устройство, сенсорный экран.*

Для распознавания изображений применяются различные подходы, связанные с использованием вторичных параметров: без выделения вторичных параметров (полносвязная нейронная сеть, метод k ближайших соседей, линейная регрессия), ручное выделение вторичных параметров (метод сравнения гистограмм, метод выделения краёв, метод Виолы — Джонса), автоматическое выделение вторичных параметров (поиск по «регионам интереса», свёрточные нейронные сети). Методы, используемые без выделения вторичных параметров, дают большую ошибку распознавания, а также более низкую скорость работы. Передовым на данный момент является метод, использующий аппарат свёрточных нейронных сетей [1].

Архитектура свёрточных нейронных сетей близка строению человеческого мозга: в нём также есть области, не имеющие ярко выраженной специализации и одинаково обрабатывающие всю входящую информацию (зрительную, сенсорную, звуковую, логическую и т. д.). Одним из преимуществ свёрточных нейронных сетей является то, что признаки изображения извлекаются обособленно. Указанные сети способны находить инварианты в изображении и реагировать главным образом на них, не обращая внимания на прочий

шум. Стоит отметить достаточно большую универсальность свёрточных нейронных сетей. Эта модель может быть дополнена и расширена другими алгоритмами и методами, разрабатываемыми как в теории искусственных нейронных сетей, так и в других областях знания [2].

Классические нейронные сети плохо масштабируются для работы с изображениями ввиду полной связанности их скрытых слоев. Например, для работы с изображением (256×256×3), где 3 – число компонент цветности, только один нейрон в первом скрытом слое должен иметь 256×256×3 = 196 608 весов. Добавление скрытых слоев в такой сети приводит к значительному увеличению числа параметров, что, в свою очередь, зачастую приводит к переобучению сети. [3]

Слои сверточной сети имеют такие характеристики как глубина, высота и ширина (рис. 1).

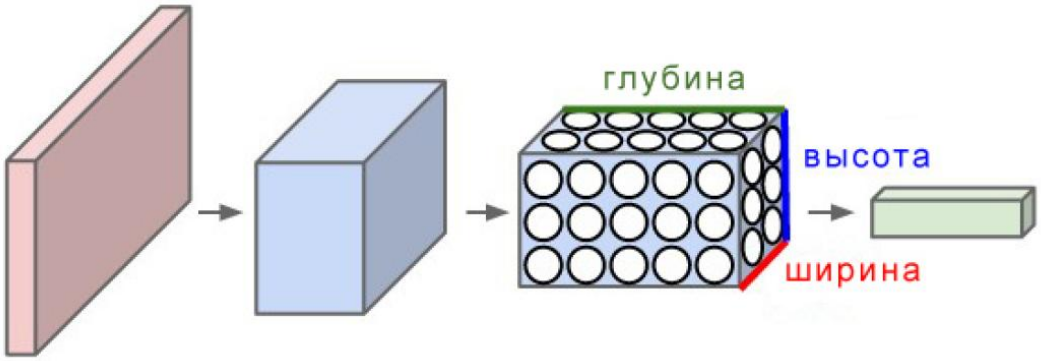

Рис. 1. Визуализация сверточной нейронной сети в трехмерном пространстве

С математической точки зрения, такая архитектура позволяет уменьшить количество параметров сети, что позволяет улучшить обобщающие свойства сети. Кроме того, такая архитектура позволяет извлекать локальные свойства из входных данных.

Процесс обучения и свертки интерпретируются следующим образом:

1. Фильтры первого запоминают общие свойства, характерные для входных данных.

2. Фильтры последующих слоев запоминают характерные комбинации свойств, полученных предшествующими слоями.

3. С возрастанием глубины слои извлекают все более глубокие связи между свойствами, характерными для каждого класса входных данных [4].

Исходя из того, что фильтр, полученный для одного участка изображения, может быть применен и на другом, с целью понижения числа обучаемых весов применяется разделение параметров между нейронами одного фильтра. Например, для сверточного слоя (256×256×96) и рецептивного поля (5×5×3) потребуется всего 96 × (5×5×3) = 7 200 чисел, в то время как полносвязанному слою потребовалось бы (256×256×96) × (5×5×3) = 471 859 200 весов для хранения коэффициентов каждого пикселя. Фильтр используется для всего изображения и требует гораздо меньшее количество настраиваемых весов [3]. Таким обра-

зом, применение свёрточных нейронных сетей позволяют строить сложные иерархии признаков и выявлять более тонкие закономерности в данных [5].

Блочная диаграмма сверточной нейронной сети представлена на рис. 2.

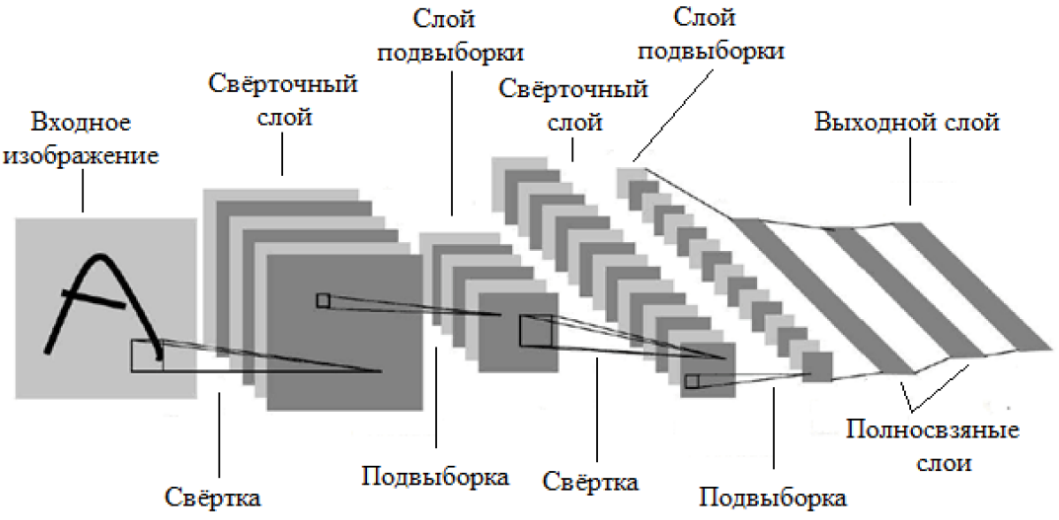

Рис. 2 Сверточная нейронная сеть

Как и другие методы машинного обучения – системы, обучающиеся из данных – сверточные нейронные сети используются для решения множества задач, которые тяжело решить с использованием стандартного логического программирования [6]. Поэтому целесообразно их использование для идентификации при реализации доступа к мобильному устройству.

В современных мобильных устройствах используются различные механизмы разграничения доступа: пароли, PIN-коды, отпечаток пальца, а также графический ключ (паттерн). Последний реализуется функцией соединения кругов (частей мобильного экрана), количество которых варьируется от 9 до 36.

Несколько лет назад норвежский исследователь Марта Логе занялась изучением графических ключей. В ходе своей работы она проанализировала 4000 вариантов паттернов и выяснила, что они могут состоять из не менее 4 точек и не более 9, а общее количество комбинаций точек составляет приблизительно 390 тысяч. М. Логе подсчитала, что 44% ключей имеют начало в верхней левой точке и 77% начинаются в каком-либо из углов поля ввода. Также она вычислила среднее количество точек в ключе – пять, а это означает, что злоумышленнику, который хочет разблокировать смартфон, в теории придется перебрать менее 8 000 комбинаций [7].

С другой стороны, таким паттерном может быть любой эскиз владельца смартфона: рисунок с уникальными областями использования экрана, скоростью движения и силы нажатии. Таким образом, объединяя классический механизм блокировки мобильного устройства и алгоритм биометрической аутентификации по сенсорному почерку, получается более устойчивая система доступа к личным данным владельца.

Кроме того, модель сверточной нейронной сети способна распознавать графические ключи пользователей, учитывая погрешности и шумы: масштабируемость отдельных частей «ключевого» изображения, смещения, повороты, смена ракурса ввода и прочее. Представляется целесообразным разработка мобильного приложения для анализа возможности применения указанного метода на реальных моделях.

Список литературы

1. Голубинский А.Н., Толстых А.А. Распознавание объектов на телевизионных изображениях с использованием аппарата свёрточных нейронных сетей // *Вестник ВИ МВД России*, 2017, №1, с.71-81.
2. Лагунов Н.А. Применение свёрточных нейронных сетей в задачах распознавания многопараметрических объектов // *Пространство и Время*, 2013, №3 (13), с.194-197.
3. Горемыкин И.В., Соловьев А.С., Бутенко Л.Н. Модели глубокого машинного обучения // *Известия ВолгГТУ*. 2016, №3 (182), с.26-32.
4. Рогаль А.А. Применение методов глубокого обучения в задаче распознавания изображений // *IN SITU,* 2016, №6, с.13-17.
5. Федотов Д.В., Сидоров М.Ю. О применении эволюционных алгоритмов для настройки нейронной сети при решении задачи распознавания эмоций // *Актуальные проблемы авиации и космонавтики*, 2016, №12. с.586-587.
6. Михалевич Ю.С., Ткаченко В.В. Использование свёрточных нейронных сетей для распознавания автомобильных номеров. Преимущества и недостатки по сравнению с шаблонным методом // *Научный журнал КубГАУ - Scientific Journal of KubSAU*, 2016, №120, с.1706-1715.
7. Сухова А.Р. Проблемы безопасности графических ключей, используемых для блокирования смартфонов // *Инновационная наука*, 2016, №2-3 (14), с.140-141.