УДК 004.0032.26

НЕКОТОРЫЕ ВОПРОСЫ ИСПОЛЬЗОВАНИЯ СВЕРТОЧНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ ДЕТЕКТИРОВАНИЯ КЛЮЧЕВЫХ ТОЧЕК НА ИЗОБРАЖЕНИИ

Баранов М. Д.
Научный руководитель – Юринок В.И., к.т.н., доцент

Целью данной работы является исследование возможности использования сверточных искусственных нейронных сетей для детектирования ключевых точек на изображении, что в дальнейшем может применяться для распознавания объектов на изображениях, а также для их сравнения. В данной работе рассмотрены основные принципы работы сверточных нейронных сетей и построение математических моделей.

Метод поиска ключевых точек давно применяется для распознавания объектов на изображении. Этот метод широко используется в сфере распознавания людей, в системах видеоаналитики. Использование нейронных сетей может сделать данный метод более точным, а также более устойчивым к различного рода искажениям, что позволит применять данный алгоритм более широко. Целью нашей работы было не только написание математической модели, которая позволит детектировать ключевые точки, но и использование в качестве выходных параметров нейронной сети не координаты ключевых точек, как это делалось ранее, а тензора вероятности нахождения данной ключевой точки в указанной координате. Данный подход позволил увеличить точность модели. Нейронная сеть была обучена на детектирование координат углов номерных знаков автомобилей. Средняя ошибка по всей валидационной выборке составила 1.25 пикселей, при скорости работы 40 миллисекунд на кадр. Так же в данной модели был реализован верификатор, который мог бы отвечать за наличие искомого объекта на подаваемом изображении. Модель была реализована на фреймворке torch7.

Подход, при котором вместо координат ключевых точек используется тензор вероятности, показал лучшей результат. Также точность работы верификатора составила 99%, что гораздо упрощает отсеивание background изображений. Подход детектирования ключевых точек с использованием нейронных сетей показывает себя как алгоритм, имеющий большой показатель точности в сочетании с быстродействием, что позволяет использовать данный алгоритм в системах интеллектуального видеонаблюдения в режиме реального времени.

Литература

1. С. Хайкин, Нейронные сети: полный курс, 2-е изд., испр. : Пер. с англ. – М.: ООО «И.Д. Вильямс», 2006, 1104 стр.

УДК 004.056.55

АЛГОРИТМЫ ШИФРОВАНИЯ, ОСНОВАННЫЕ НА ДАННЫХ

Стухальский А.Л. Романенко Р.А.
Научный руководитель – Федосик Е.А., физ.-мат. наук, доцент.

Существует большое количество алгоритмов шифрования. Многие из них устарели и не пригодны для использования. Причина в том, что производительность вычислительных систем растет экспоненциально (ЗаконМура). Причем проблемы возникают последовательно и со всех сторон: с увеличением производительности уменьшается время взлома, а для усиления алгоритмов применяются все более сложные методы, которые требуют больших вычислительных затрат.

Самым востребованным и распространенным алгоритмом шифрования на протяжении длительного периода времени является Advanced Encryption Standard (AES). Тем не менее надежность AES вызывает сомнения в связи с его простым математическим описанием.

Для решения возникающих проблем, авторами разработана концепция динамических алгоритмов. Для простоты понимания концепции можно воспользоваться теорией систем (ЧерныйЯщик). Всю систему можно представить, как «черный ящик» со входом и выходом. Сама реализация «черного ящика» также представляется в виде набора «черных ящиков». Анализируя каждую часть в отдельности можно обнаружить элементы с простой зависимостью по отношению к другим. Авторы предлагают представлять подобные элементы в качестве самостоятельных логических частей. Такой подход имеет много преимуществ, главным из которых является гибкость системы. Заменяя один или несколько элементов системы либо их порядок на выходе получаем новую систему. Примечательно, что наличие нескольких заменяемых элементов увеличивает сложность взлома. Несмотря на то, что структура системы не изменилась, результат полученной криптосистемы будет кардинально отличатся от предыдущего. Теория систем позволяет рассмотреть альтернативный подход: вместо замены частей системы можно внести в систему изменчивые элементы. Поведение такого элемента зависит от его текущего состояния.