ОТЗЫВ

на автореферат диссертации Перова Артёма Андреевича «Универсальный метод построения решающих правил с использованием сверточных нейронных сетей для анализа генераторов псевдослучайных последовательностей на основе итеративных блочных шифров», представленной на соискание учёной степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики»

Анализ автореферата А.А. Перова показывает, что в своей диссертационной работе автор нашёл интересное применение свёрточных нейронных сетей для обнаружения закономерностей и отклонений от случайности в псевдослучайных последовательностях, генерируемых на основе итеративных блочных шифров. Действительно, современные свёрточные нейросетевые модели в целом и выбранная исследователем модель Inception ResNet-v2 в частности достигли впечатляющих результатов в распознавании графических изображений, а выходные последовательности итеративных генераторовмогут быть легко представлены в виде растровых эквивалентов.

Большую значимость имеет тот факт, что разработанный Перовым А.А. метод генерации решающих правил является достаточно универсальным и имеет перспективу быть развитым в общий подход к анализу любых итеративных генераторов псевдослучайных последовательностей.

Работа имеет высокую теоретическую и практическую ценность, её результаты могут найти своё широкое применение, например, в задачах обеспечения безопасности использования информационных технологий.

Заметно то, что диссертационное исследование является не только теоретическим, но и содержит солидную практическую компоненту. Например, весьма впечатляет размер списка проанализированных генераторов на основе блочных шифров, для каждого из которых для разных номеров раундов подсчитаны значения процента верных решений нейронной сети при различении соседних раундов. Предлагаемые автором новые методы и алгоритмы реализованы в виде программного обеспечения с использованием современных ИТ-технологий.

Стоит также отметить весьма широкий спектр конференций и семинаров, где докладывались результаты данной научной работы и производилась её апробация.

При знакомстве с авторефератом появился ряд замечаний и вопросов, представленных ниже. Все перечисленные вопросы и замечания не являются критичными для научной и практической ценности работы и в большей своей части имеют характер пожеланий автору на его дальнейшие исследования.

1. В автореферате приведены такие архитектурные параметры нейронной сети, как размерность ядер свёртки в разных частях сети, а также параметры слоёв подвыборки. Если данные параметры определены выбранной использованной моделью, то возникает вопрос – проводились ли эксперименты для более точной подстройки вышеперечисленных параметров для достижения лучших результатов обучения для данной конкретной задачи? Подстраивались ли иные макропараметры модели?
2. Сказано, что преобразование анализируемой псевдослучайной последовательности в изображение заключается в последовательном присваивании компонентам палитры RGB значений,считываемых байт.Возникает вопрос, связанный с выбором именно такого принципа преобразования. Данный вопрос является скорее идеей попробовать и сравнить иные способы перехода от последовательности к растровому эквиваленту.
3. Предложение «Утилита выполняет конвертацию текстового файла (или опционально – потоковой последовательности) в BMP файл с глубиной 24 бита, где каждая компонента палитры RGB кодируется 8 битами (палитра содержит 256 цветов)» требует уточнения, связанного с тем, что при 24-битном размере палитра содержит 224 = 16777216 цветов, а каждый компонент палитры – 256 оттенков.
4. Из автореферата недостаточно чётко вытекает ответ на вопрос, связанный с возможностью практического обучения свёрточной нейронной сети, в ходе которого производится запоминание основных паттернов, характерных для генерируемых последовательностей при разном числе раундов. Какова должна быть вычислительная мощность ЭВМ для того, чтобы обучение производилось за практически приемлемое время?
5. Название таблицы 1 «значения правильных решений нейронной сети» недостаточно точно отражает её содержимое. Скорее, это «значения процента верных решений нейронной сети при различении соседних раундов генераторов».

Исходя из всего вышеизложенного, можно заключить, что диссертация А.А. Перова является самостоятельным, обоснованным и завершенным научным исследованием, полностью удовлетворяет требованиям ВАК, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.17 "Теоретические основы информатики". Данное исследование отличается научной новизной и

соответствует паспорту специальности, а автор заслуживает присуждения искомой степени кандидата технических наук.

Доцент кафедры «Прикладные информационные технологии» Института прикладных информационных технологий и коммуникаций (ИнПИТ), кандидат технических наук — Кузьмин Алексей Константинович

Адрес: 410054, г. Саратов, ул. Политехническая, 77, Саратовский государственный технический университет имени Гагарина Ю.А.
E-mail: kuz_alex_konst@mail.ru
Телефон: 8-962-62-11-431

Подпись Кузьмина А.К. удостоверяю
Начальник управления кадров
М.Н. Висюлькина
12.03.2021 г.

УПРАВЛЕНИЕ КАДРОВ