искусственной нейронной сети. В работе был использован многослойный перцептрон с двумя скрытыми слоями. На первом слое 90 нейронов, на втором – 20. Результаты обучения сети показали возможность успешного детектирования до 70 % случаев наличия информации, скрытой в графических изображениях с использованием трех выбранных стегоалгоритмов.

Литература

1. Абденов А.Ж., Леонов Л.С. Использование нейронных сетей в слепых методах обнаружения встроенной стеганографической информации в цифровых изображениях // Ползуновский вестник. 2010. № 2. С. 221–225.

ВОССТАНОВЛЕНИЕ ЗАШУМЛЕННОГО ТЕКСТА С ПОМОЩЬЮ ГЕНЕРАТИВНО-СОСТЯЗАТЕЛЬНЫХ СЕТЕЙ

М.А. Кадан

Генерирующие состязательные сети (GAN, Generative Adversarial Networks) [1] явились эффективной моделью в создании контента с помощью методов искусственного интеллекта. Особенность GAN в том, что они обучаются создавать синтетические данные, подобные эталонным данным. Классическим примером использования GAN является построение сети, которая анализируя изображения рукописных цифр, учится генерировать новые изображения с нуля – по сути, в этом случае мы учим сеть «писать».

В работе ставилась задача обучения GAN способности «читать» искаженную текстовую информацию. Предполагается, что мы располагаем набором цифровых изображений плохого качества (подготовленных при отсутствии оптической стабилизации, плохой резкости, в условиях плохой освещенности, низкой разрешающей способности и т.д.), содержащих текстовую информацию. Необходимо добиться путем обучения GAN улучшения качества таких искаженных текстов, которое позволит восстановить текст.

В качестве эталонного множества было использовано множество печатных латинских букв, представляющих различные компьютерные шрифты. Была сформирована обучающая выборка, включающая примеры написания отдельных латинских букв. Обучающая выборка представлена набором битовых аналогов для графических монохромных изображений: буквы размером 20×20 пикселей вписаны в квадрат 28×28 и отцентрированы вокруг центра масс.

Проведенный эксперимент позволил сгенерировать на основе зашумленных текстов более 25000 букв, которые модель ACGAN (Auxiliary Classifier Generative Adversarial Network) [2] посчитала неотличимыми от букв, представленных в обучающей выборке. Несмотря на использование производительной вычислительной системы, эксперимент потребовал значительных временных затрат.

Литература

1. Generative Adversarial Networks / Ian J. Goodfellow [et al.]. arXiv:1406.2661.

2. Augustus Odena, Christopher Olah, Jonathon Shlens. Conditional Image Synthesis With Auxiliary Classifier GANs. arXiv:1610.09585.

РАЗРАБОТКА СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ ВТОРЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ ПАРАЛЛЕЛЬНОГО ПРОГРАММИРОВАНИЯ И ТЕХНОЛОГИЙ ОТКАЗОУСТОЙЧИВОСТИ

Камил Ихаб Абдулджаббар Камил, М.Б. Абросимов

Системы предотвращения вторжений – это программные или аппаратные системы сетевой и компьютерной безопасности, которые обслуживают распределенные информационные системы, обнаруживают информационные вторжения или нарушения политик безопасности и автоматически защищают от подобных нарушений. Ввиду роста номенклатуры информационных угроз и сокращения времени реализации внешних вторжений для распределенной вычислительной системы возникает необходимость в сокращении времени выявления и противодействия всей номенклатуре информационных угроз. Поскольку при самых неблагоприятных реализациях информационных угроз от распределенных

информационных систем требуется соблюдение надежности и безотказности, то данные условия обеспечиваются преимущественно за счет аппаратного и программного резервирования. Пусть дана распределенная информационная система, для которой необходимо обосновать состав и технические параметры подсистем резервирования (в рамках технологии отказоустойчивости) и определить параметры системы предотвращения вторжений. Для данной информационной системы моделируются экстремальные режимы функционирования по внешним и внутренним рабочим нагрузкам, а также вся известная номенклатура внешних информационных угроз. В отсутствии системы предотвращения вторжений, аппаратного и программного резервирования информационной системы отмечаются снижения эффективности ее функционирования при сочетании предельных значений диапазона рабочих нагрузок и реализаций всей номенклатуры внешних угроз. Экспериментальным путем подбираются параметры алгоритма управления параллельными вычислениями системы предотвращения вторжений на уровне данных и решаемых задач, благодаря которым добиваются своевременного определения угроз и выбора эффективных мер по противодействию им. Пострадавшие в результате реализации информационных угроз элементы информационной системы заменяются на время их восстановления на резервные элементы, которые функционировали до этого в зеркальном режиме, но без коммуникации со внешними абонентами информационной системы. Эффективность защитных мероприятий за период моделирования определяется как отношение предотвращенного ущерба информационной системе (в денежных единицах) к сумме стоимостей системы предотвращения вторжений и технологии отказоустойчивости с учетом аппаратного и программного резервирования информационной системы. По результатам имитационного моделирования обосновываются требования к системе предотвращения воздействий с параллельными вычислениями и к составу системы аппаратного и программного резервирования, реализующей технологию повышения отказоустойчивости.

ЗАЩИТА ИНФОРМАЦИИ С ПОМОЩЬЮ ТЕХНОЛОГИИ NFC

Ю.С. Камышев, Ю.А. Скудняков

Одним из современных способов защиты информации является NFC (Near field communication) – коммуникация ближнего поля либо ближняя бесконтактная связь. Это технология беспроводной передачи данных малого радиуса действия, которая дает возможность обмена данными между устройствами, находящимися на близком расстоянии; анонсирована в 200 4г. Эта технология является простым расширением стандарта бесконтактных карт, которое объединяет интерфейс смарт-карты и считывателя в единое устройство. Устройство NFC может поддерживать связь и с существующими смарт-картами, и со считывателями стандарта ISO 14443, и с другими устройствами NFC и, таким образом, совместимо с существующей инфраструктурой бесконтактных карт, уже использующейся в общественном транспорте и платежных системах. NFC нацелена прежде всего на использование в цифровых мобильных устройствах. NFC – это беспроводная дистанционная технология, которая работает на расстоянии не более 10 сантиметров. NFC работает на частоте 13,56 МГц. NFC всегда включает инициатор и цель. Инициатор активно генерирует радиочастотное поле, которое может влиять на пассивную цель. Также возможна NFC-связь между двумя устройствами при условии, что оба устройства включены [1]. Но у данной технологии есть и минусы, например, эксплойт 0day, подслушивание (так как это радиосигнал), модификация данных (например, устройствами глушения RFID), атака с использованием ретрансляции и т.д. Исходя из вышеизложенного, можно сделать вывод о том, что NFC на сегодняшний день является весьма небезопасным протоколом, с помощью которого в том числе и передаются банковские данные. В связи с этим риск потерять деньги весьма велик. На сегодняшний день это самая распространенная технология в данном сегменте и остается только надеяться, что платежные данные не попадут третьим лицам.

Литература

1. Near Field Communication (NFC) Technology and Measurements [Электронный ресурс]. – URL: www.rohde-schwarz.com (дата обращения: 18.05.2018).