Литература

1. Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption) << Cost(Signature) + Cost(Encryption) // Crypto'97. 1997.

2. Barbosa M., Farshim P. Certificateless Signcryption // ACM symposium on Information, computer and communications security. 2008.

РЕШЕНИЕ ЗАДАЧ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ИСПОЛЬЗОВАНИЕМ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ

Н.А. Искров, Д.В. Лящук

В докладе представлен обзор наиболее актуальных угроз информационной безопасности (ИБ) и основных направлений использования искусственных нейронных сетей (ИНС) при решении задач обеспечения ИБ. Описаны основная теория построения ИНС и их принцип работы.

Наиболее актуальные угрозы по мнению специалистов в области ИБ: внедрение в сеть предприятия вирусного ПО; простота реализация и распространенность DDoS-атак; снижение эффективности автоматизированных методов защиты от спама; сложности в поиске и идентификации уязвимостей ИБ; возникновение новых способов вторжения. Поэтому следует обратить внимание на перспективные методы защиты информации, в частности, на теорию ИНС.

Преимущества ИНС в решении задач ИБ: в процессе обучения ИНС могут быть выявлены новые сведения, закономерности, использование которых возможно для коррекции топологии сети, входных данных, для получения более эффективной защиты; после обучения ИНС входной сигнал становится нечувствительным к небольшим колебаниям при правильном построении архитектуры ИНС и верном выборе качества обучения; ИНС способна обратить внимание на те сведения, которые являются несущественными для интеллектуальной системы защиты.

Основные направления внедрения ИНС в защиту информации: обнаружение вторжений и защита от DDoS-атак; криптографические методы защиты информации, автоматизация процессов криптоанализа; проведение испытаний подсистем и оборудования систем защиты, моделирование возникновения внештатных ситуаций; прогрозирование шаблонных данных с целью выявления аномалий в классификации или кластеризации операций.

ДЕТЕКТИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ СЛЕПЫМ МЕТОДОМ

А.М. Кадан, И.А. Сазановец

Стеганографические методы позволяют скрыть одну информацию, сообщение, в другой, контейнере. В работе в качестве контейнеров рассматриваются изображения. Для реализации стеганографического сокрытия информации существует множество алгоритмов. И, зная использованный в конкретном случае стегоалгоритм, можно написать программу детектирования скрытого сообщения. В работе рассмотрен метод детектирования стеганографической информации в случаях, когда алгоритм сокрытия неизвестен. Такие способы в стегоанализе называются слепыми. И их использование возможно благодаря тому факту, что внедрение информации в контейнер оставляет после себя искажения.

Решаемая задача является задачей бинарной классификации, так как нужно, имея некое изображение, определить, содержит ли оно скрытое сообщение или нет. Для ее решения предлагается использовать методы машинного обучения. Исходное изображение раскладывается на три цветовых канала: красный, зеленый и синий. Для каждого канала строится трехуровневое двумерное вейвлет-разложение (используется вейвлет-функция Хаара) [1]. Из полученных коэффициентов разложения берутся аппроксимационный, вертикальные и диагональные коэффициенты. В частотных плоскостях этих коэффициентов вычисляются моменты третьего и четвертого порядков (коэффициент асимметрии и эксцесс). Полученные моменты рассматриваются как данные входного вектора (dataset’a) для работы

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