Списокиспользованныхисточников:
1. An Introduction to different Types of Convolutions in Deep Learning. [Электронный ресурс] – Режим доступа: https://towardsdatascience.com/types-of-convolutions-in-deep-learning-717013397f4d. – Дата доступа : 12.03.2017.
2. Mobile Real-time Video Segmentation. [Электронный ресурс] – Режим доступа: https://research.googleblog.com/2018/03/mobile-real-time-video-segmentation.html. – Дата доступа: 12.03.2017.
3. MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications. [Электронный ресурс] – Режим доступа: https://arxiv.org/abs/1704.04861. – Дата доступа: 09.03.2017.
4. Batch Normalization: Accelerating Deep Network Training by Reducing Internal Covariate Shift. [Электронный ресурс] – Режим доступа: https://arxiv.org/abs/1502.03167. – Дата доступа: 12.03.2017.
5. The Marginal Value of Adaptive Gradient Methods in Machine Learning. [Электронный ресурс] – Режим доступа: https://arxiv.org/abs/1705.08292. – Дата доступа: 09.03.2017.

МЕССЕНДЖЕР С ВАРИАТИВНОСТЬЮ ИСПОЛЬЗОВАНИЯ КРИПТОСИСТЕМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Матюшонак А.Д., Валетко А.Н., Ковалёва Н.В., Ширяев Т.С.
Стройникова Е. Д. – ассистент кафедры информатики

В современном мире большинство информации передаётся через интернет, где её без особого труда можно перехватить, в связи с этим всё больше развиваются и способы её защиты. Самым простым и популярным из них является внедрение различных криптосистем.

Криптосистема – это комплексная модель, состоящая из алгоритмов шифрования и дешифрования, текстов различного объёма и содержания.

В зависимости от типа использованных алгоритмов криптосистемы соответственно делятся на симметричные, асимметричные и смешанные, в которых используются алгоритмы обоих типов. Так, при использовании симметричных криптосистем сообщение шифруется и дешифруется одним ключом, поэтому собеседникам нужно заранее договориться об используемом ключе. В асимметричных криптосистемах используются закрытый и открытый ключи. Открытый ключ пересылается от получателя к отправителю, который с помощью открытого ключа зашифрует сообщение, а получатель дешифрует сообщение с помощью закрытого ключа, который известен лишь ему.

Наибольшая производительность достигается при использовании симметричных методов шифрования, их скорость на несколько порядков выше, длина используемого ключа также заметно меньше, однако зачастую возникают трудности с безопасной передачей ключа. В связи с этим более предпочтительным является использование смешанных криптосистем. В данных криптосистемах сообщение шифруется симметричным способом, отправляется получателю, после чего асимметричным методом отправляется ключ.

Ввиду существования риска перехвата и изменения сообщения после его отправки принято использовать цифровую подпись. Для её создания необходимо вычислить хеш-функцию текста или файла, после чего полученное значение зашифровать с использованием секретного асимметричного ключа отправителя и добавить полученную строку к исходному тексту. Для того чтобы удостовериться в подлинности полученного сообщения, необходимо расшифровать хеш-функцию с использованием открытого ключа отправителя и повторно вычислить хеш-функцию исходного текста. Если обе функции совпадают, делается вывод о сохранности исходного сообщения.

С целью достаточной защиты пользовательских сообщений было разработано приложение Safend, использующее при отправке сообщений смешанную криптосистему и цифровую подпись. Пользователь может комбинировать уже имеющиеся в программе методы симметричного шифрования, произвольно выбирая для них порядок и входные данные, таким образом создавая собственный метод шифрования.

Для реализации данной цели был выбран язык программирования C#, т. к. он располагает большим количеством библиотек асимметричного шифрования, удобен в сетевом использовании для отправки и получения зашифрованных сообщений, а также является кроссплатформенным, что позволит в будущем перенести программу и на мобильные системы.

Переписка может осуществляться как между двумя пользователями, так и в групповом виде. Для переписки между двумя абонентами требуется добавить пользователя в список контактов, указав его ip и дав имя контакту, после чего его можно будет выбрать и начать переписку. Для групповой переписки необходимо, чтобы один из пользователей стал сервером, вызвав в программе соответствующую функцию, после к нему можно будет подключиться, указав его ip.

При добавлении пользователя в контакты создаётся случайный симметричный шифр, который отправляется ему по алгоритму RSA. При получении данный шифр будет сохранён как у получателя, так и у отправителя. В дальнейшем при их переписке по умолчанию будет использоваться именно это шифрование. Однако при желании пользователь может зашифровать сообщение собственным симметричным ключом, который будет отправлен по алгоритму RSA.

Таким образом, при переписке может быть использовано вплоть до трёх уровней защиты информации, и для того, чтобы удостовериться в том, что сообщение не было перехвачено и изменено, может быть прикреплена цифровая подпись. Подобный подход обеспечивает необходимый уровень защиты информации, передаваемой посредством сети интернет.

Список использованных источников:

1. Шифрование [Электронный ресурс]. – Режим доступа: https://professorweb.ru/my/csharp/base_net/level2/2_3.php. – Дата доступа: 08.04.2018.
2. Криптографические методы и средства защиты информации [Электронный ресурс]. – Режим доступа: http://itsphera.ru/it/cryptographic-methods-and-tools-for-information-protection.html. − Дата доступа: 08.04.2018.

ПРИМЕНЕНИЕ РЕКУРСИВНЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА ТОНАЛЬНОСТИ ТЕКСТА

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Витковский А.В.

Жвакина А. В. – к. т. н, доцент

Современные порталы в сети Интернет позволяют пользователям высказывать свое мнение о различных предметах, событиях, явлениях. Эти мнения могут быть полезными для различных исследований, необходимых аналитикам, SMM-специалистам, бренд-менеджерам, PR-агентам и иным специалистам, нуждающимся в получении агрегированной информации. Таким образом существует необходимость в инструментах для анализа отзывов пользователей. Пользователи оставляют свои комментарии в интернете на естественных языках, таких как английский, русский и др., что является проблемой для обработки программными средствами. В работе рассматривается такой метод обработки естественного языка, как анализ тональности текста.

Обработка естественного языка (Natural Language Processing, NLP) − общее направление искусственного интеллекта и математической лингвистики. Оно изучает проблемы компьютерного анализа и синтеза естественных языков. Одной из задач, решаемых в рамках обработки языка, является анализ тональности текста. Анализ тональности текстов – это класс методов анализа содержания, предназначенный для классфикации автоматического распознавания в тексте лексики с эмоциональной окраской, а также мнений (эмоциональных оценок) автора об объектах, которые упоминаются в тексте.

Для решения задачи анализа тональности текста применяют нейронные сети. Искусственные нейронные сети (НС) — совокупность моделей биологических нейронных сетей. Представляют собой сеть элементов — искусственных нейронов — связанных между собой синаптическими соединениями. Сеть обрабатывает входную информацию и в процессе изменения своего состояния во времени формирует совокупность выходных сигналов. Работа сети состоит в преобразовании входных сигналов во времени, в результате чего меняется внутреннее состояние сети и формируются выходные воздействия. Обычно НС оперирует цифровыми, а не символьными величинами. Искусственные нейронные сети — набор математических и алгоритмических методов для решения широкого круга задач. Алгоритмы на основе машинного обучения показывают свою эффективность в задачах обработке естественных языков.

Большинство систем прогнозирования настроений работают по простому алгоритму, рассматривая слова в изоляции, давая положительные баллы для положительных слов и отрицательные баллы для отрицательных слов, а затем суммирует баллы. Таким образом, порядок слов игнорируется и теряется важная информация. Однако, модели на основе нейронных сетей фактически создают представления целых предложений, основанные на структуре предложения. Они вычисляют тональность, основанную на том, как слова влияют значение более длинных фраз. Таким образом, модель на основе нейронных сетей не так легко обмануть, как обычные алгоритмы.

Наиболее часто используемыми в исследованиях методами являются методы на основе машинного обучения с учителем. Сутью таких методов состоит в том, что сначала нейронная сеть получает коллекцию из данных и уже готовых точных решений, и в процессе машинного обучения сеть настраивается, и далее уже на других данных может выдавать нужные результаты.

Для решения задачи анализа тональности могут использоваться рекурсивные нейронные сети. Рекурсивные нейронные сети (англ. Recursive neural network; RvNN) − вид нейронных сетей, работающих с данными переменной длины. Модели рекурсивных сетей используют иерархические структуры образцов при обучении. Например, изображения, составленные из сцен, объединяющих подсцены, включающие много объектов. Выявление структуры сцены и её деконструкция − нетривиальная задача. При этом необходимо как идентифицировать отдельные объекты, так и всю структуру сцены. В рекурсивных сетях нейроны с одинаковыми весами активируются рекурсивно в соответствии со структурой сети. В процессе работы рекурсивной сети вырабатывается модель для предсказания для структур переменной размерности, так и скалярных структур через активацию структуры в соответствии с топологией. Рекурсивные нейронные сети успешно применяются при обучении последовательных структур и деревьев в задачах обработки естественного языка, при этом фразы и предложения моделируются через векторное представление слов. Рекурсивные сети первоначально появились для распределённого представления структур, используя