Министерство образования Республики Беларусь

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Факультет прикладной математики и информатики

Кафедра математического моделирования и анализа данных

Волков Евгений Сергеевич

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА И СИНТЕЗА КРИПТОГРАФИЧЕСКИХ АЛГОРИТМОВ

Курсовой проект
студента 3 курса 9 группы

«Допустить к защите»

Руководитель работы

Мальцев Михаил Владимирович
Доцент
Кафедра математического
моделирования и анализа данных

_____

«_____» _____ 2021 г

Минск 2021

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

За последние несколько лет наблюдается повышение интереса к нейронным сетям. Нейронные сети вошли в практику везде, где нужно решать задачи прогнозирования, классификации или управления. Нейронные сети являются исключительно мощным методом моделирования, позволяющим воспроизводить чрезвычайно сложные зависимости. Именно поэтому искусственные нейронные сети постепенно внедряются в качестве инструмента для анализа и синтеза криптографических алгоритмов.

Первая глава представляет собой введение в нейронные сети. Будет рассмотрена структура нейронных сетей, их виды, как происходит обучение нейронных сетей.

Вторая глава раскрывает возможности практического применения нейронных сетей в повседневной жизни. Рассмотрены такое области применения, как проектирование и оптимизация сетей связи, распознавание речи, управление ценами и производством, анализ потребительского рынка и исследование спроса, анализ страховых рисков, обслуживание кредитных карт, медицинская диагностика, обнаружение классификаций, оценка недвижимости и распознавание символов.

В третьей главе будет рассказано о применении нейронных сетей в криптографии: создание синтетических отпечатков пальцев для обучения биометрических систем безопасности, создание криптографических ключей с высокой энтропией на основе биометрических данных, генерация хеш-функций.

В четвёртой главе описано применение нейронных сетей в криптоанализе. Использование нейронных сетей в криптоанализе позволяет исследовать криптографические алгоритмы, проводить атаки на криптосистемы, исследовать их надёжность и устойчивость.

Глава 1 ВВЕДЕНИЕ В НЕЙРОННЫЕ СЕТИ

1.1 Определение и структура нейронной сети

Нейронная сеть (искусственная нейронная сеть) — математическая модель, а также её программное или аппаратное воплощение, построенная по принципу организации и функционирования биологических нейронных сетей — сетей нервных клеток живого организма. Это понятие возникло при изучении процессов, протекающих в мозге, и при попытке смоделировать эти процессы. После разработки алгоритмов обучения получаемые модели стали использовать в практических целях: в задачах прогнозирования, для распознавания образов, в задачах управления и др.

Биологический нейрон состоит из ядра, дендритов, по которым принимаются импульсы от других нейронов, и единственного аксона, по которому передаётся импульс. Аксон соединён с дендритами других нейронов через синапсы – специальные образования, которые влияют на передаваемый импульс. Большое количество соединённых вместе нейронов образуют нейронную сеть.

В основе искусственных нейронных сетей лежит такой же принцип. Нейроны соединены между собой в один или несколько слоёв, на вход они получают N входных значений x_i, умножают их на соответствующие веса ω_{ij} и добавляют смещение b_j. По своей сути, веса – мера влияния данного входного значения на состояние нейрона. Далее применяется функция активации f(x), которая определяет выходное значение по входным значениям. Пример нейронной сети показан на Рисунке 1.2, где Act – некая функция активации.

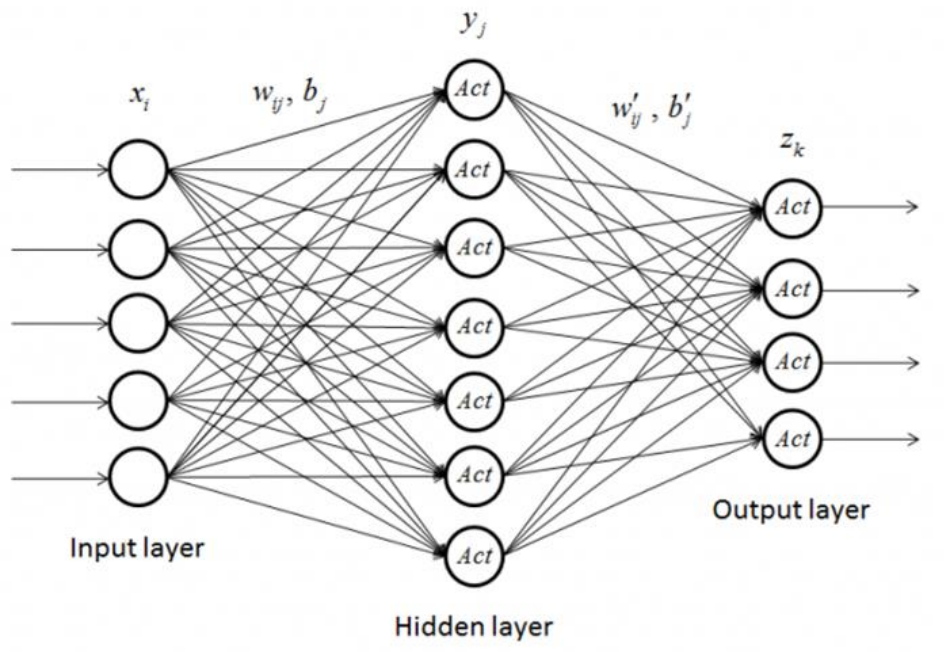

Рисунок 1.2 – Пример нейронной сети

Архитектура нейронной сети, т.е. количество слоёв и нейронов в них, определяется особенностями и сложностью конкретных задач. Однако на практике невозможно создать нейронную сеть с огромным количеством нейронов и слоёв ввиду ограниченности ресурсов.

Нейронные сети могут быть полносвязными (каждый нейрон предыдущего слоя соединён с каждым нейроном следующего слоя), свёрточными, рекуррентными, трансформерами (комбинация свёрточных и рекуррентных).

Основной идеей работы искусственных нейросетей является то, что они обучаются, а не программируются. Т.е. во время обучения на некоторых данных основная цель нейронной сети – подстроить свои веса таким образом, чтобы уменьшить ошибки по заранее заданному критерию.

1.2 Функции активации

Рассмотрим некоторые функции активации:

1) Ступеньчатая (пороговая) функция: $f(x) = \begin{cases} 1, x \geq \alpha, \\ 0, x < \alpha. \end{cases}$

Применяется при бинарной классификации (объект принадлежит одному из двух классов: “1” – принадлежит, “0” – не принадлежит, α – порог).

2) Сигмоида: $f(x) = (1 + e^{-x})^{-1}$.

Множество значений данной функции – [0,1], т.е. любое значение нейрона на выходе можно отобразить на этот отрезок. Этот факт используют при решении задач классификации.

3) Softmax: $f(x)_i = e^{x_i} \Big/ \sum_{j=1}^{N} e^{x_j}$.

Данная функция преобразует вектор с компонентами x_i в вектор с компонентами $f(x)_i$, значения которых лежат на отрезке [0,1] и сумма которых равна 1. Другими словами, функция показывает вероятность принадлежности каждому из N классов.

4) ReLU: $f(x) = \max(0, x)$.

На первый взгляд кажется, что функция линейна, но ReLU, как и их комбинация, нелинейна. Это позволяет использовать её в нейронных сетях со множеством слоёв. Ещё один плюс данной функции – разреженость активации. В силу определения функции, в нейросетях с большим количеством нейронов количество используемых нейронов будет меньше, чем при использовании других функций активации.

1.3 Обучение нейронной сети

Выделяют два типа обучения: “с учителем” и “без учителя”.

При обучении “без учителя” нейронная сеть на вход получает данные без ответов (например, при решении задачи кластеризации или оптимизации). Цель алгоритма – подстроить веса так, чтобы при схожих входных данных получались схожие выходные данные. В процессе обучения выделяются статистические особенности входных данных, на основе которых они [данные] группируются в классы.

При обучении “с учителем” на вход нейронной сети подаются данные для обучения вместе с правильными ответами. В этом случае можно задать критерий, по которому будут считаться ошибки предсказания нейронной сети. По выбранному алгоритму идёт изменение весовых коэффициентов до тех пор, пока ошибка не будет на довольно низком уровне.

Математически это можно описать так: в процессе обучения нейросетью формируется выходной сигнал y, реализующий некоторую функцию g(x). Пусть решение задачи – функция y = f(x), заданная входными парами (x^i, y^i). Обучение состоит в поиске некоторой функции g, близкой к f, минимизируя ошибку ε. Выбирая функцию потерь, получаем задачу многомерной оптимизации.

Существует много различных как способов задания ошибки (MSE – среднеквадратическая ошибка, SSE – суммарная квадратическая, CrossEntropy и др.), так и методов решения задачи оптимизации (метод градиентного спуска, метод Нестерова и др.).

Глава 2 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ НЕЙРОННЫХ СЕТЕЙ

Потенциальными областями применения искусственных нейронных сетей являются те, где человеческий интеллект малоэффективен, а традиционные вычисления трудоёмки или физически неадекватны (т. е. не отражают или плохо отражают реальные физические процессы и объекты). Актуальность применения нейронных сетей многократно возрастает, когда появляется необходимость решения плохо формализованных задач. Основные области применения нейронных сетей: автоматизация процесса классификации, автоматизация прогнозирования, автоматизация процесса распознавания, автоматизация процесса принятия решений; управление, кодирование и декодирование информации; аппроксимация зависимостей и др.

Промышленность		
Управление технологическими процессами	Идентификация химических компонент	Контроль качества артезианских вод
Оценка экологической обстановки	Прогнозирование свойств синтезируемых полимеров	Управление водными ресурсами
Оптимальное планирование	Разработка нефти и газа	Управление работой пресса
Идентификация вида полимеров	Управление ценами и производством	Оптимизация работы моторов
Обнаружение повреждений	Оптимизация закупок сырья	Контроль качества изделий
Приложения аналитической химии	Анализ проблем функционирования заводов и магазинов	Прогнозирование потребления энергии
Высокие технологии		**Оборона**
Проектирование и оптимизация сетей связи	Идентификация и верификация говорящего	Анализ визуальной аэрокосмической информации
Анализ и сжатие изображений	Видеонаблюдение	Отбор целей
Распознавание печатных и рукописных символов	Автоматизированное распознавание речевых команд	Обнаружение наркотиков и взрывчатых веществ
Фальсификации в пищевой и парфюмерной пром-сти	Распознавание слитной речи с (и без) настройки на говорящего	Сличение изображений с криминальной базой данных
Обслуживание кредитных карт	Речевой ввод текста в компьютер	Предсказание целесообразности условного освобожден.
Наука и техника		**Здравоохранение**
Поиск неисправностей в научных приборах	Спектральный анализ и интерпретация спектров	Идентификация микробов и бактерий
Диагностика печатных плат	Интерпретация показаний сенсоров	Диагностика заболеваний
Идентификация продуктов	Моделирование физических систем	Интерпретация ЭКГ
Синтез новых видов стекла	Анализ данных в ботанике	Анализ качества лекарств
Автоматизированное проектирование	Планирование химических экспериментов	Обработка и анализ медицинских тестов
Оптимизация биологических экспериментов	Отбор сенсоров для контроля химических процессов	Прогнозирование результатов применения методов лечения
Геофизические и сейсмологические исследования	Прогноз температурного режима технологических процессов	Оптимизация атлетической подготовки
Распознавание ингредиентов	Диагностика сбоев сигнализации	Диагностика слуха
Бизнес и финансы		
Выбор сбытовой политики	Прогноз прибыли (Cash-flow)	Прогнозирование продаж
Принятие административных решений	Предсказание и расшивка «узких мест»	Анализ целей маркетинговой политики
Предсказания на фондовой бирже	Прогноз эффективности кредитования	Прогнозирование экономических индикаторов
Анализ финансового рынка	Прогнозирование валютного курса	Анализ страховых исков
Исследование фактора спроса	Прогнозирование и анализ цен	Отбор перспективных кадров
Моделирование бизнес-стратегии	Построение макро- и микроэкономических моделей	Стратегии в области юриспруденции
Предсказание наступления финансовых кризисов	Предсказание необходимых трудодней для реализации проекта	Оценка и прогнозирование стоимости недвижимости

Таблица 1 – Области применения нейронных сетей

2.1 Проектирование и оптимизация сетей связи

С помощью нейронных сетей успешно решается важная задача в области телекоммуникаций – нахождение оптимального пути трафика между узлами. Учитываются две особенности: во-первых, решение должно быть адаптивным, т. е. учитывать текущее состояние сети связи и наличие сбойных участков, а во-вторых, оптимальное решение необходимо находить в реальном времени. Кроме управления маршрутизацией потоков, нейронные сети используются для получения эффективных решений в области проектирования новых телекоммуникационных сетей.

2.2 Распознавание речи

Распознавание речи – одна из наиболее популярных областей применений нейронных сетей. Демонстрационная система для диктороно-независимого речевого управления встроенным калькулятором Windows (Российская компания Нейропроект) способна распознавать 36 команд, сказанных в стандартный микрофон. Для классификации слов используется двухкаскадная иерархическая нейронная сеть, где первый каскад состоит из одного персептрона (1000 входов, 24 нейрона в скрытом слое, 6 выходов), а второй каскад – из 6 персептронов с различными параметрами слоев. При этом первый персептрон осуществляет грубое распознавание слова, относя его к одному из 6 классов; роль второго каскада – точно классифицировать команду внутри класса. Для построения данной нейронной сети используется библиотека NeuroWindows, а также специальный алгоритм иерархического обучения. В обучении сети принимали участие 19 дикторов.

2.3 Управление ценами и производством

Часто недооцениваются потери от неоптимального планирования производства. В связи с тем, что спрос и условия реализации продукции зависят от времени, сезона, курсов валют и многих других факторов, то и объем производства должен гибко варьироваться с целью оптимального использования ресурсов. Нейросетевая система (компания Neural Innovation Ltd.), предназначенная для планирования затрат при издании газет, обнаруживает сложные зависимости между затратами на рекламу, объемами продаж, ценой, ценами конкурентов, днем недели, сезоном и т.д. В результате использования системы осуществляется выбор оптимальной стратегии издательства с точки зрения максимизации объема продаж или прибыли.

2.4 Анализ потребительского рынка

Один из популярных маркетинговых механизмов – распространение купонов, дающих право покупки определенного товара со скидкой. Так как затраты на рассылку купонов довольно велики, решающим фактором является

эффективность рассылки, то есть повышение доли клиентов, воспользующихся скидкой. Для повышения эффективности купонной системы необходимо проведение предварительной сегментации рынка, а затем адресация клиентам каждого сегмента именно тех купонов, которыми они с большей вероятностью воспользуются. Нейросетевая система (компания IBM Consulting), прогнозирующая свойства потребительского рынка пищевых продуктов, решает задачу кластеризации с помощью сетей Кохонена. На втором этапе для потребителей каждого из кластеров подбираются подходящие коммерческие предложения, а затем строится прогноз объема продаж для каждого сегмента. Другой популярный маркетинговый механизм – распространение поощрительных товаров (когда, например, присылая 5 этикеток от кофе, клиент бесплатно получает кружку). Здесь, обычные методы прогнозирования отклика потребителей могут быть недостаточно точны иногда, спрос на кружки оказывается слишком велик, и многие покупатели годами ждут получения приза. Прогнозирующая нейросетевая система (компания GoalAssist Corp.) использует сеть с адаптивной архитектурой нейросимулятора NeuroShell Classifier (компании Ward Systems Group). На входы данной нейронной сети, применяемой для классификации возможных откликов потребителей, подаются различные параметры товаров и рекламной политики для разделения входов на 4 вида откликов. Те же входы вместе с ответом первой сети подаются на вход сети нейросимулятора NeuroShell Predictor (компании Ward Systems Group), предназначенной для решения задачи количественного прогнозирования. При этом средняя ошибка предсказаний эффекта от распространения поощрительных товаров составляет всего около 4,0 %.

2.5 Исследование спроса

Для сохранения бизнеса в условиях конкуренции компании приходится поддерживать постоянный контакт с потребителями – «обратную связь». Крупные компании проводят опросы потребителей, позволяющие выяснить, какие факторы являются для них решающими при покупке данного товара или услуги, почему в некоторых случаях предпочтение отдается конкурентам и какие товары потребитель хотел бы увидеть в будущем. Анализ результатов такого опроса – достаточно сложная задача, так как существует большое количество коррелированных параметров. Нейросетевая система (компания Neural Technologies) позволяет выявлять сложные зависимости между факторами спроса, прогнозировать поведение потребителей при изменении маркетинговой политики, находить наиболее значимые факторы и оптимальные стратегии рекламы, а также очерчивать сегмент потребителей, наиболее перспективный для данного товара. В частности, система применяется для исследований

предпочтений различных сортов пива в зависимости от возраста, дохода, семейного положения потребителя и других параметров.

2.6 Анализ страховых исков

Нейросетевая система Claim Fraud Analyser (компания Neural Innovation Ltd.) предназначена для выявления в реальном времени подозрительных страховых исков, поступающих в связи с повреждениями автомобилей. На входы системы подаются такие параметры, как возраст и опыт водителя, стоимость автомобиля, наличие подобных происшествий в прошлом и др. В результате обработки такой информации нейронная сеть определяет вероятность того, что данный иск не связан с мошенничеством. Система позволяет не только обнаруживать фальсификации, но и улучшать отношения с клиентами за счет более быстрого удовлетворения справедливых исков.

2.7 Обслуживание кредитных карт

Нейросетевая система Falcon (компания HNC), разработанная для отслеживания операций с краденными кредитными картами и поддельными чеками, позволяет по частоте сделок и характеру покупок выделить подозрительные сделки и сигнализировать об этом в контролирующие службы. Благодаря данной системе, отслеживающей более 260 миллионов счетов 16 крупнейших эмитентов кредитных карт, потери банков от таких операций заметно уменьшились. Аналогичная система (компания ITC), используемая для обработки операций с кредитными картами VISA, предотвратила в 1995 г. нелегальные сделки на сумму более 100 млн долларов.

2.8 Медицинская диагностика

Система объективной диагностики слуха у грудных детей (Российская компания НейроПроект) обрабатывает зарегистрированные "вызванные потенциалы" (отклики мозга), проявляющиеся в виде всплесков на электроэнцефалограмме, в ответ на звуковой раздражитель, синтезируемый в процессе обследования. Обычно, для уверенной диагностики слуха ребенка опытному эксперту-аудиологу необходимо провести около 2000 тестов, что занимает около часа. Система на основе нейронной сети способна с той же достоверностью определить уровень слуха уже по 200 наблюдениям в течение всего нескольких минут, причем без участия квалифицированного персонала.

2.9 Обнаружение фальсификаций

Подсчитано, что потери бюджета США от мошенничеств и фальсификаций в области здравоохранения составляют около 730 млн долларов в год. Тестирование системы обнаружения (стоимость – 2,5 млн долларов, компания ITC) показало, что нейронная сеть позволяет обнаруживать 38,0%

мошеннических случаев, в то время как существовавшая ранее экспертная система – только 14,0 %.

2.10 Оценка недвижимости

Стоимость квартиры или дома зависит от большого числа факторов, таких как общая площадь, удаленность от центра, экологическая обстановка, престижность, тип дома, и т.д. Так как вид этих зависимостей неизвестен, то стандартные методы анализа неэффективны в задаче оценки стоимости. Как правило, эта задача решается экспертами-оценщиками, работающими в агентстве по недвижимости. Недостатком такого подхода субъективность оценщика, а также возможные разногласия между различными экспертами. Система на основе нейронной сети (компания Attrasoft) способна эффективно решать широкий спектр задач объективной оценки стоимости недвижимости, в частности, с учетом 13 факторов при оценке стоимости домов в г. Бостон (США). Группа исследователей из университета г. Портсмут (Великобритания) в системе на основе нейронной сети использовала данные по оценке недвижимости из обзоров риэлтеровских фирм и списков аукционных цен. Результаты исследования показали, что система делает оценки стоимости близкие к оценкам лучших экспертов и специалистов данного профиля.

2.11 Распознавание символов

Распознавания букв и символов, с одной стороны – одна из наиболее разработанных и освещенных в специальной литературе проблем, а с другой – не смотря на кажущуюся простоту, чрезвычайно трудно реализуемая на практике задача. Рассмотрим особенности применения нейронной сети (компания AT&T Bell Laboratories) при сортировке писем на почте в г. Баффало, США. Задача состоит в применении нейросетевых методов при разработке системы распознавания рукописных цифр, которые отправители писем указывали на конвертах в качестве индекса. Исследовались две строчки индексов: первые – написанные быстро и, как правило, неразборчиво, и вторые – написанные более тщательно печатными буквами. Разработчики наполнили базу данных более 9000 символами, переведенных с конвертов, которые прошли через почтовую службу г. Баффало в 1988 г. На Рисунке 2.1 показаны некоторые почтовые индексы (вверху) и уже изолированные цифры, подготовленные для распознавания (внизу). Видно, что индексы пишутся крайне неразборчиво, так что сотрудники почты считают, что некоторые отправители в действительности не желают, чтобы их письма доходили по назначению. В связи с этим, к сожалению, большинство подобных систем распознавания обладают точностью 95,0%, что является едва приемлемым показателем. В целом ряде случаев, наиболее трудная проблема при распознавании символов – не собственно

распознавание, а обнаружение символов и выяснение их местоположения, т.е. – верная интерпретация индекса, состоящего из известного количества позиций, изолирование и подготовка к распознаванию отдельных цифр индекса. Поэтому для простоты будем полагать далее, что процесс распознавания начинается уже после изолирования цифры.

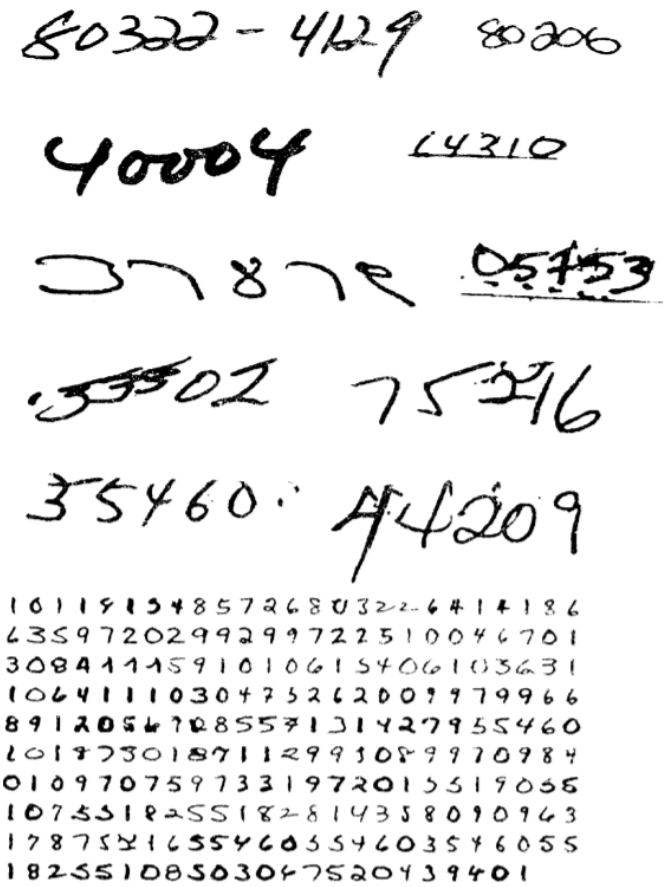

Рисунок 2.1 - Рукописные индексы, обрабатываемые почтовой службой г.Баффало (вверху) и взятые из них отдельные изолированные цифры (внизу)

Рукописные индексы, обрабатываемые почтовой службой г. Баффало (вверху) и взятые из них отдельные изолированные цифры (внизу) Для каждой цифры разработчики строили решетку (сетку) размерностью 16 х 16 пикселей. В ходе исследований в 1988 г. было выяснено, что применение стандартного подхода, основанного на применении обученной нейронной сети обратного распространения к сырому массиву пикселей и чисел, приемлемого результата не дает. В 1988-1990 гг. был предложен метод локализации информативных участков, вокруг которых строились решетки 5 х 5 и 7 х 7 пикселей, после чего на вход нейронной сети обратного распространения поступал 180- мерный вектор. Конечная нейросетевая система распознавания представляет собой аппаратный модуль, реализованный на базе ПЦОС и соединенный с ПК. Обучение нейронной сети системы проводится единожды, однако достаточно

медленно с использованием 167693 представительских выборок. Ошибка системы в процессе распознавания символов – 0,14 % при предъявлении обучающей пары из набора представительских выборок, использованной при обучении, и 5,0 % при распознавании «новых» символов. Таким образом, разработчики и пользователи приняли решение о приемлемости результатов и необходимости использования системы для предварительной сортировки конвертов.

Глава 3 НЕЙРОННЫЕ СЕТИ И КРИПТОГРАФИЯ

3.1 Общие сведения

Различные методы машинного обучения представляют собой интересную область исследований с огромным потенциалом применения. Одной из сфер является криптография. Ещё в 1991 году Рональд Ривест, один из создателей RSA, выступил на ASIACYPT'1991 с приглашенным докладом о криптографии и машинном обучении. В своем докладе Ривест обсудил сходства и различия между машинным обучением и криптографией, а также то, как каждая область может повлиять на другую. С тех пор как Рональд Ривест заговорил о "взаимообогащении" областей машинного обучения и криптографии, эта область привлекла к себе огромное внимание [6].

Можно выделить две основные области применения машинного обучения в криптографии:

1) Создание криптосистем на основе машинного обучения
2) Классификация зашифрованного трафика

3.2 Применения в криптографии

В 2002 году Михал Розен-Цви предложил использовать взаимное обучение в древовидном автомате чётности в качестве криптосистемы с открытым ключом. В статье объясняется, как древовидный автомат чётности может быть использован в качестве криптосистемы с открытым ключом путем использования его состояния синхронизации в качестве ключа в определенном правиле шифрования и дешифрования. Этим "ключом" можно обмениваться публично, без необходимости предварительной коммуникации. Принимающей стороне необходимо выполнить лишь конечное число шагов обмена входами-выходами для достижения сходимости к состоянию синхронизации [6].

В 2005 году было представлено новое явление, названное взаимным обучением. Это явление взаимного обучения может быть использовано в криптографии. Взаимное обучение может помочь двум сторонам коммуникации создать общий секретный ключ через открытый канал. Обе стороны имеют преимущество перед атакующим в том, что атакующий будет обучаться односторонне, что сделает практически невозможным создание такого же секретного ключа, который будет у обеих сторон.

В 2007 году обсудили возможности соединения машинного обучения и криптографии. В статье говорится, что на техническом уровне существуют тесные связи между методами машинного обучения и методами, используемыми в криптографии. В качестве примера была рассмотрена техника "Boosting", которая является методом машинного обучения, предназначенным для

извлечения как можно большей мощности из алгоритма обучения. Это может быть связано с методами усиления криптосистем.

В 2009 году Аль-Шаммари и Зинсир-Хейвуд представили метод классификации, основанный на машинном обучении, для классификации зашифрованного трафика. Работа была выполнена для оценки надежности классификации зашифрованного трафика с помощью машинного обучения. Работа была сфокусирована на потоке без использования широко используемых характеристик, таких как адреса InterNet Protocol (IP), номера портов и информация о полезной нагрузке. Результаты исследования показали, что алгоритм обучения C4.5 превзошел другие алгоритмы, такие как RIPPER, Naive Bayesian, support vector machine и AdaBoost [6].

В 2011 году был представлен доклад о состязательном машинном обучении. В докладе шла речь о таксономии для классификации атак на онлайновые алгоритмы машинного обучения. Кроме того, в докладе были рассмотрены уязвимости алгоритмов машинного обучения и меры борьбы с ними. В статье также представлены два способа моделирования возможностей противников. В статье подробно рассмотрен особый тип атак, получивший название разведывательных атак на целостность. В этом типе атак противник пытается пассивно обойти механизм обучения, чтобы использовать "слепые пятна" в обучающемся, которые позволяют злоумышленникам оставаться незамеченными. Этот тип атак может быть использован в различных приложениях машинного обучения.

В 2012 году вышла книга с подборкой идей по использованию машинного обучения в стеганализе. В книге описаны способы применения машинного обучения в борьбе со стеганографией. Основная идея заключалась в классификации объектов на стеганограммы или чистые документы с использованием возможностей машинного обучения классификации.

Graepel в 2012 году представили систему, с помощью которой можно делегировать выполнение алгоритма машинного обучения вычислительному сервису, сохраняя при этом конфиденциальность благодаря использованию схемы гомоморфного шифрования с выравниванием. Смысл этого подхода заключался в использовании более высокопроизводительных вычислительных сервисов, таких как облачные вычисления, для повышения скорости машинного обучения и возможности обработки больших объемов данных [6].

В 2014 году появился алгоритм шифрования с симметричным ключом, основанный на сети встречного распространения. Предложенный алгоритм представляет собой симметричный блочный шифр, в котором данные преобразуются в биты и пропускаются через нейронную сеть в качестве текста, а в качестве выхода рассматривается результирующий результат процесса

обучения без наблюдения. Несмотря на то, что принцип работы не был четко изложен в статье, это направление может быть изучено в дальнейшем.

В 2015 году были представлены три основных протокола классификации, которые опираются на машинное обучение при классификации зашифрованных данных. В результате работы были получены классификаторы, сохраняющие конфиденциальность. Предложенные классификаторы были протестированы на медицинских наборах данных и доказали, что достигают правильной классификации с удовлетворительной эффективностью.

3.3 Схема регенерации криптографического ключа на основе мультибиометрии

В данном разделе рассматривается схема регенерации криптографического ключа на основе мультибиометрии [7]. Она представляет собой многоинстанционную систему, объединяющую информацию от левой и правой радужных оболочек глаз человека. Даугман показал, что левая и правая радужки человека не коррелируют и поэтому могут рассматриваться как два независимых источника биометрической информации. Извлекается отличительная информация из изображений радужной оболочки глаза пользователя в виде кодов радужной оболочки. Изображение радужки разлагается с помощью фильтров Габора, а квантованная фазовая информация используется для построения кода радужки. Объединяются коды радужки, полученные из изображений обоих глаз пользователя, чтобы получить комбинированный мультибиометрический вектор признаков. Более того, предлагается новый подход к объединению информации в области признаков с помощью взвешенной коррекции ошибок, который помогает улучшить производительность. Наконец, вводится ключ перестановки (защищенный паролем), что позволяет повысить точность, конфиденциальность и безопасность системы.

Рассмотрим подробно предлагаемую мультибиометрическую систему регенерации ключей. Основная структура этой схемы аналогична схеме Хао (Рисунок 3.1). Хорошо известно, что коды радужки, полученные из различных изображений радужки одного и того же пользователя, содержат вариации, которые в данной работе называются ошибками. Существует два типа ошибок в кодах радужки:

(1) фоновые ошибки, вызванные шумом камеры, эффектами захвата изображения и т.д., и

(2) ошибки всплеска, которые являются результатом зеркальных отражений, окклюзий.

Для борьбы с этими ошибками используются коды с коррекцией ошибок (ECC).

Генерируется случайная битовая строка K, которая присваивается пользователю и затем кодируется с помощью кодов Рида-Соломона (RS), выход которых далее кодируется кодами Хадамарда. Коды Хадамарда исправляют фоновые ошибки, а коды RS исправляют ошибки всплеска. Выход кодера называется псевдокодом S. Для того чтобы справиться с каскадной структурой двух ECC, количество битов в каждом символе RS и во входных словах кодов Хадамарда устанавливается равным 7 (m = 7). Эталонный код радужки I_{ref}(или, в общем случае, вектор биометрических признаков в двоичной форме) переписывается с помощью операции XOR с S для получения заблокированного шаблона кода радужки I_{lock}. На этапе регенерации ключа другой код радужной оболочки I_{test} (тестовый код радужной оболочки) переписывается с помощью операции XOR с I_{lock}. Эти операции через XOR переносят ошибки в кодах радужки на псевдокод. Если количество ошибок находится в пределах возможностей коррекции ошибок ECC, ошибки исправляются частью декодера ECC и регенерируется ключ K', который совпадает с K. Если ошибок больше, регенерированный ключ $K' \neq K$.

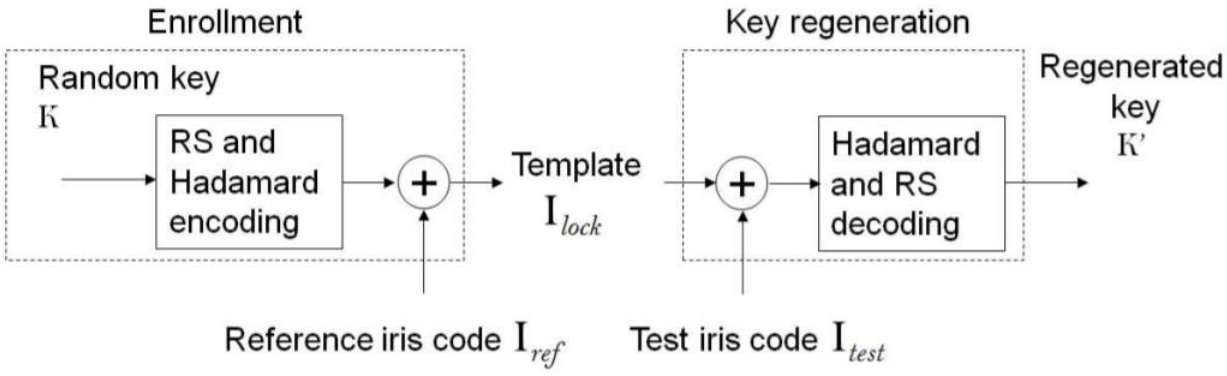

Рисунок 3.1 – Схема системы регенерации криптографического ключа на основе биометрии

В схеме ECC на (Рисунок 3.1) существует два уровня коррекции ошибок: на первом уровне коды Хадамарда исправляют до $2^{(k-1)} - 1$ ошибок в 2^k-битном блоке. Если блок имеет больше, чем $2^{(k-1)} - 1$ ошибок, этот блок декодируется неправильно и приводит к ошибке. Второй уровень ECC состоит из RS-кодов. Выход этапа декодирования Хадамарда служит входом для этапа декодера RS. RS-коды исправляют ошибки, вызванные неправильным декодированием кодами Хадамарда, и генерируют ключ K'.

3.4 Автоматическая генерация синтетических отпечатков пальцев

Отпечатки пальцев человека часто используются в различных приложениях для аутентификации и идентификации, начиная от "умных" дверей и заканчивая авторизацией платежей на мобильных телефонах. Оценка производительности и надежности систем идентификации и верификации на основе отпечатков

пальцев требует доступа к большой базе данных отпечатков пальцев. Однако на практике получение огромного массива изображений отпечатков пальцев сопряжено с большими затратами. Во многих случаях исследовательские группы, разрабатывающие системы аутентификации по отпечаткам пальцев, не имеют доступа к большой общедоступной базе данных. Производительность этих систем напрямую зависит от качества и количества доступных данных.

В дополнение к вышеперечисленным препятствиям, сбор отпечатков пальцев большого количества людей вызывает серьезные проблемы с конфиденциальностью и безопасностью. В случае взлома отпечатки пальцев многих пользователей будут напрямую доступны злоумышленникам и могут быть использованы для обмана любых других систем аутентификации, принимающих отпечатки пальцев. С этой целью мы изучаем задачу создания синтетических отпечатков пальцев, которые могут решить вышеупомянутые проблемы.

Синтетические отпечатки пальцев решают проблему доступности, поскольку они могут быть сгенерированы практически для любого количества образцов. Более того, синтетические отпечатки пальцев генерируются искусственно, поэтому они не передают никакой информации о реальной личности. Синтетические отпечатки пальцев играют важную роль и в других задачах. Например, их можно использовать для анализа устойчивости системы верификации к троянским атакам. Для проведения такого анализа необходимо большое количество отпечатков пальцев, где их тонкие особенности можно варьировать, фиксируя другие характеристики, такие как ориентация изображения.

Предыдущие решения по созданию синтетических отпечатков пальцев были способны либо создавать синтетические шаблоны микроособенностей отпечатков пальцев, либо синтетические изображения реальных отпечатков пальцев, но с низким разрешением. Решения, основанные на математических моделях отпечатков пальцев, страдают от недостатка энтропии и обобщения до точного распределения вероятностей реальных отпечатков пальцев.

Предыдущие решения, основанные на моделях глубокого обучения (DL), также не могут создавать высококачественные изображения из-за малого объема доступных реальных отпечатков пальцев для обучения этих моделей.

Однако была разработана система SYNFI, новая комплексная структура для автоматической генерации высококачественных синтетических отпечатков пальцев в масштабе. Это решение формулирует процесс создания синтетических отпечатков пальцев как две параллельные задачи глубокого обучения, основанные на парадигме генеративной адверсарной сети (GAN) и суперразрешения (SR) [8]. В частности, SYNFI формализует и удовлетворяет

следующим целям проектирования, чтобы соответствовать ожиданиям реального мира:

- генерируемые образцы должны сохранять миниатюрные характеристики отпечатков пальцев, используемых в системах аутентификации, например, структуру гребней, раздвоения и окончания гребней.
- Идеальная система должна быть способна генерировать полные отпечатки пальцев, а не частичные.
- Синтетические отпечатки пальцев должны быть вычислительно неотличимы от реальных отпечатков, чтобы их можно было использовать как средство повышения безопасности биометрических систем хранения данных.
- Система должна быть полностью автоматизирована, не требуя ручной разработки признаков, и иметь высокую масштабируемость.

Основные этапы работы SYNFI:

1) Генерация синтетических отпечатков низкого качества с помощью GAN. Большинство отпечатков имеют разрешение 256*256. Однако процедура обучения GAN опирается на изображения с меньшим разрешением. Поэтому для обучения GAN используется база данных низкого качества (LQD). Однако модель SR нуждается в базе данных высокого качества (HQD). Поэтому сперва обучается GAN для создания низкокачественных синтетических отпечатков пальцев.
2) Обобщение на высококачественные изображения. На втором этапе SYNFI низкокачественное изображение преобразуется в изображение высокого разрешения с детальной структурой.

3.5 Генерация хэш-функции с помощью нейронной сети

Эффективная генерация хэш-функции очень важна для достижения безопасности современных сетей. *Криптографическая хэш-функция* – это преобразование, которое принимает входные данные и возвращает значение фиксированного размера, которое называется хэш-значением. Искусственная нейронная сеть (ИНС), как возможный подход, может быть использована для генерации хэш-функции.

Функция F является *односторонней функцией*, если ее определение общеизвестно и не требует секретной информации для своей операции. Для любого заданного x легко вычислить F(x). Для заданного y в диапазоне F трудно найти x такой, что F(x)=y.

Рассмотрим вариант генерации односторонней хэш-функции. *Односторонняя хэш-функция* – это функция H, которая отображает сообщение произвольной длины M в массив фиксированной длины MD. MD является

односторонней хэш-функцией, если она односторонняя и для заданных M и H(M) трудно найти сообщение M'≠M такое, что H(M')=H(M) [4].

Рассмотрим структуру нейронной сети для генерации хэш-функций.

Количество нейронов входного слоя равно 512 и соответствует 512 битам входного сообщения, которое хэшируется многослойной сетью с прямой связью. Количество нейронов скрытого слоя является целью оптимизации. Количество нейронов выходного слоя равно 128, что соответствует количеству битов хэш-функции. Структура многослойной feed-forward сети для вычисления хэш-функции показана на Рисунке 3.5. Вход в ИНС представлен 512-битным сегментом входных данных от сообщения. Остальные входные нейроны представлены 128 битами из предыдущего вычисления хэш-функции и используются на следующем шаге. Количество скрытых слоев и количество нейронов в скрытых слоях является целью оптимизации. Выходной слой состоит из 128 битов вычисленной хэш-функции [5].

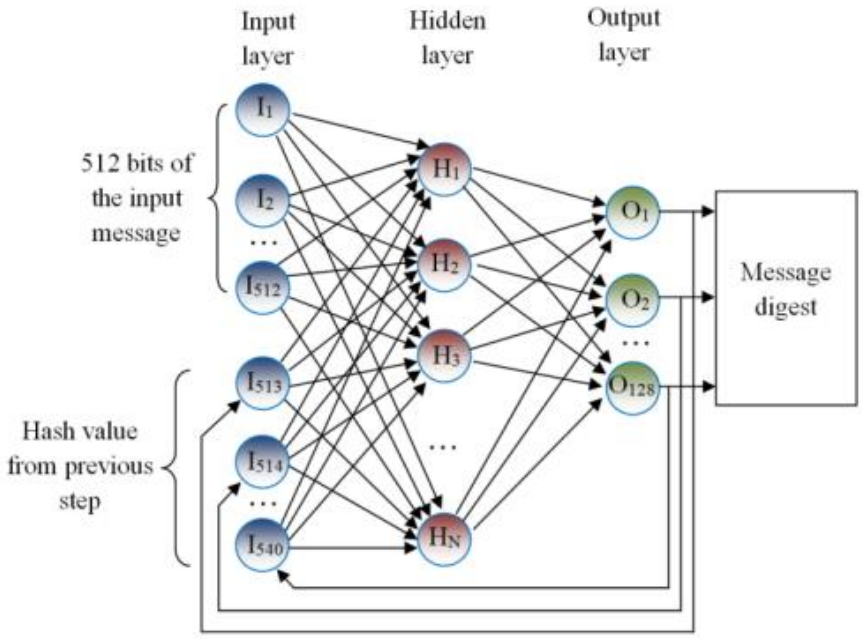

Рисунок 3.5 – Строение многослойной сети

Вычисление хэш-функции можно разделить на три этапа. Первый шаг начинается с преобразования сообщения в последовательность битов. Эта последовательность битов разбивается на блоки длиной 512 бит. Если в сообщении меньше 512 бит или после разбиения сообщения последний блок меньше 512 бит, то добавляется прокладка.

Второй этап начинается с генерации начального значения дайджеста сообщения, которое используется как вход для вычисления хэш-функции (128 бит). Эта операция выполняется только на первом шаге вычисления, поскольку у нас еще нет хэш-значения. После выполнения первого шага хэш-значение используется на следующем шаге вычисления вместе со следующим 512-битным

блоком массива. На рис. 2 показано, как 128-битное хэш-значение используется в качестве входа в нейронную сеть. Параметры искусственной нейронной сети генерируются на том же шаге. Параметры нейронной сети – это значения весов между слоями сети и значения смещения каждого нейрона. Их количество фиксировано и не изменяется в процессе работы нейронной сети.

После этого на третьем шаге можно отправлять блок за блоком сообщения на вход искусственной нейронной сети. Вычисление хэш-функции завершается, когда все блоки сообщения обработаны. Последнее значение на выходе ИНС является конечным значением хэш-функции.

Глава 4 НЕЙРОННЫЕ СЕТИ И КРИПТОАНАЛИЗ

4.1 Общие сведения о нейрокриптоанализе

Нейронный криптоанализ – использование глубокого обучения для проведения атак на криптографические структуры (системы, алгоритмы и т.д.).

С увеличением вычислительной мощности нейронный криптоанализ становится более реальным вариантом для проведения атак на более сложные шифры.

Наиболее развитой областью нейроприкладного криптоанализа является атака на сторонние каналы. Противник получает физические свойства, такие как уровень мощности сигнала на целевой аппаратной реализации криптосистемы. Глубокое обучение используется для более эффективного анализа таких метрик, как временные характеристики и информация об амплитуде мощности, полученых от аппаратного обеспечения [3].

Методы машинного обучения применяются для проведения атак через сторонние каналы. В 2011 году Хосподар представил первое исследование, в котором предлагалось использовать машинное обучение в атаках на сторонние каналы. В предложенной системе использовался алгоритм обучения с использованием машины опорных векторов наименьших квадратов (LS-SVM), сторонним каналом было энергопотребление, а целью была программная реализация стандарта расширенного шифрования (AES). Исследование показало, что выбор параметров алгоритма машинного обучения сильно влияет на результаты [6].

Еще одно сопряжение сторонних каналов и машинного обучения было опубликовано в 2014 году. Лерман, Бонтемпи и Маркович предложили использовать методы машинного обучения для повышения точности атак на сторонние каналы. Поскольку атаки сторонних каналов опираются на физические измерения аппаратных реализаций криптосистем, всегда существуют определенные параметрические предположения, на которые опираются эти атаки. Предлагаемое использование машинного обучения позволяет ослабить такие допущения и работать с векторами признаков высокой размерности.

В 2012 году Алани представил атаку "известный текст", которая использует нейронную сеть для проведения криптоанализа. Предложенная атака обучает нейронную сеть расшифровывать шифртекст без знания ключа шифрования. Эта атака позволила значительно сократить время и количество известных пар "открытый текст-шифртекст", необходимых для шифрования по стандартам Data Encryption Standard (DES) и Triple-DES, по сравнению с другими атаками "известный текст" [6].

В продолжение работы, ранее представленной Алани, Джаячандиран реализовал аналогичную атаку на легкий шифр Simon. Однако на этот раз атака была направлена на поиск ключа, а не открытого текста. Предложенная нейронная сеть была протестирована на версии шифра с уменьшенным тактом, а также на версии с полным тактом. Конфигурации сети также были изменены, чтобы попытаться найти максимально возможную точность.

В 2015 году было опубликовано исследование по анализу зашифрованного сетевого трафика Android. Этот анализ был направлен на выявление действий пользователя, несмотря на то, что они были зашифрованы. В данном исследовании противник не взаимодействует активно с целью, а подслушивает зашифрованный трафик. Собранный зашифрованный трафик затем анализируется с помощью передовых методов машинного обучения, чтобы выяснить действия, совершенные пользователем. Предложенная система достигла точности до 95% в определении действий пользователя.

В 2016 году Магреби и др. опубликовали свое исследование об использовании глубокого обучения в атаках по сторонним каналам. В работе рассматривается возможность использования более сложных методов профилирования для повторного использования предположений в шаблонных атаках. В этой работе методы глубокого обучения были использованы для получения более точных результатов при атаках по сторонним каналам на AES. Результаты, приведенные в статье, подтвердили преимущества этой техники, реализованной на защищенных и незащищенных реализациях AES.

4.2 Криптоанализ блочного шифра

Далее рассмотрим несколько сценариев атак на блочные шифры с помощью нейронного криптоанализа.

Большинство атак на блочные шифры осуществляется с точки зрения “чёрного ящика”, т.е. предполагается, что противник знает все спецификации алгоритмов блочных шифров, но не знает секретный ключ и соответствующие тактовые ключи [3].

Такие атаки называются атаками на восстановление ключа.

- Получив пару открытого текста и шифртекста (p, c), удовлетворяющую c=Enc(k, p), атакующий пытается найти k. В качестве обучающих данных даются тройки из случайного открытого текста, случайного ключа и соответствующего шифртекста (k_i, p_i, c_i) такого, что c_i=Enc(k_i, p_i).
- Атака на восстановление ключа с фиксированным ключом аналогична атаке на восстановление ключа, однако в качестве обучающих данных даются только пары случайных открытых текстов и соответствующих шифртекстов (p_i, c_i), таких, что c_i= Enc(k,p_i). Отдельная модель глубокого обучения не может быть сквозным решением, поскольку ключ не предоставляется в обучающих данных. Поэтому атака обычно интегрируется с методом анализа, который требует знания алгоритма. Стандартный подход заключается в угадывании ключа и исследовании работы модели для каждого возможного ключа.

Атаки на эмуляцию (подражание) шифра – это попытки имитировать алгоритм шифрования или дешифрования целевого шифра [3].

- Атака восстановления открытого текста. Учитывая шифртекст c, атакующий пытается угадать биты соответствующего открытого текста p так, чтобы c=Enc$_k$(p) с неотрицательным преимуществом. Случайные пары открытого текста и соответствующего шифртекста (p_i, c_i) такие, что c_i=Enc(k_i, p_i), даются в качестве обучающих данных.
- Атака побитового восстановления открытого текста. Атака восстановления открытого текста может быть также развернута по отдельным битам открытого текста. В качестве обучающих данных вместо (p_i, c_i) даются пары $(p_i[k], \mathrm{c}_i)$, где $p_i[k]$- k-й бит открытого текста p_i.
- Атака эмуляции шифрования. Учитывая открытый текст p, атакующий пытается угадать биты соответствующего шифртекста c так, чтобы c=Enc$_k$(p) с неотрицательным преимуществом. Случайные пары открытого текста и соответствующего шифртекста (p_i, c_i) такие, что c_i=Enc(k_i, p_i), даются в качестве обучающих данных.

ЗАКЛЮЧЕНИЕ

В первой главе были рассмотрены основные определения и понятия нейронных сетей: структура нейронных сетей, их виды, как происходит обучение нейронных сетей.

Во второй главе были изучены области практического применения нейронных сетей в повседневной жизни: распознавание речи, анализ страховых рисков, обслуживание кредитных карт, медицинская диагностика, обнаружение классификаций, оценка недвижимости и распознавание символов.

Далее были рассмотрены области применения нейронных сетей в криптографии и создание криптографических система и алгоритмов с помощью нейронных сетей, а именно, генерация хеш-функций, создание синтетических отпечатков пальцев, генерация криптографических ключей на основе биометрических данных, а также в криптоанализе, т.е. использование возможностей глубокого обучения для исследования криптосистем: атаки на сторонние каналы с использованием нейронных сетей, разные сценарии атак на блочные шифры при помощи нейросетей.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Галушкин, А. И. Нейронные сети: основы теории / А. И. Галушкин. — Москва: Горячая линия-Телеком, 2017. — 496 с.
2. Элементарное введение в технологию нейронных сетей с примерами программ / Тадеусевич Р. [и др.]; перевод с польск. И.Д. Рудинского. – М.: Горячая линия-Телеком, 2011. – 408 с.
3. Baek, S., Kim, K.: Recent Advances of Neural Attacks against Block Ciphers. In: 2020 Symposium on Cryptography and Information Security. IEEE (2020).
4. Turčaník, M., Javurek, M.: Hash Function Generation by Neural Network. In: 2016 New Trends in Signal Processing (NTSP). IEEE (2016).
5. Lian, S., Sun, J., Wang, Z.: One-way Hash Function Based on Neural Network. In: Journal of Information Assurance and Security, (2006).
6. Alani, M. M.: Applications of Machine Learning in Cryptography: A Survey. In: 2019 Proceedings of the 3rd international conference on cryptography, security and privacy, (2019).
7. Kanade, S., Petrovska-Delacretaz, D., Dorizzi, B.: Multi-Biometrics Based Cryptographic Key Regeneration Scheme. In: IEEE 3rd International Conference on Biometrics: Theory, Applications and Systems, (2009).
8. Sadegh Riazi, M., Chavoshian, S. M., Koushanfar, F.: SYNFI: Automatic Synthetic Fingerprint Generation. In: ACR Cryptology ePrint Archive, (2020).
9. Функции активации нейросети: сигмоида, линейная, ступенчатая, ReLu, tahn [Электронный ресурс]. - Режим доступа: https://neurohive.io/ru/osnovy-data-science/activation-functions/. - Дата доступа: 12.12.2021.
10. Обучение нейронной сети [Электронный ресурс]. - Режим доступа: https://neuronus.com/theory/nn/238-obucheniya-nejronnoi-seti.html. - Дата доступа: 12.12.2021.
11. Нейронная сеть [Электронный ресурс]. - Режим доступа: https://ru.wikipedia.org/wiki/Нейронная_сеть. - Дата доступа: 12.12.2021.
12. Нейронные сети [Электронный ресурс] // Большая российская энциклопедия. - Режим доступа: https://bigenc.ru/technology_and_technique/text/4114009. - Дата доступа: 12.12.2021.