УДК 004.932.2

РАЗВИТИЕ И ОЦЕНКА НЕЙРОСЕТЕВЫХ МЕТОДОВ ВЕРИФИКАЦИИ СОБСТВЕННОРУЧНОЙ ПОДПИСИ

Мискевич П.Л., магистрант гр.256241, Петровец В.Н., магистрант гр.256241, Раловец А.А., магистрант гр.256241

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

Волорова Н.А. – канд. техн. наук, доцент

Аннотация. Рукописная подпись является уникальной биометрической характеристикой, широко используемой для подтверждения личности и согласия на различные операции. В связи с ростом киберугроз и подделок подписей возникает потребность в надежных и эффективных системах верификации подписи. В данной статье обсуждается развитие нейросетевых методов верификации собственноручной подписи, анализируются существующие подходы, выявляются проблемы и рассматриваются возможные перспективы.

Ключевые слова. Верификация подписи, нейронные сети, биометрическая аутентификация, киберугрозы, выявление подделок.

Введение. С ростом числа электронных документов и транзакций увеличилась и вероятность мошенничества с использованием поддельных подписей. Подделка подписей может привести к серьезным финансовым и правовым последствиям для жертв и организаций. В связи с этим, защита от подделок стала одним из приоритетных направлений в области кибербезопасности. Киберугрозы также стали серьезным вызовом для обеспечения надежности систем верификации подписи, так как злоумышленники могут использовать различные методы для обхода защиты и получения доступа к конфиденциальной информации.

Целью данного исследования является обзор современных методов верификации собственноручной подписи, основанных на нейросетях, анализ их преимуществ и недостатков в сравнении с классическими методами машинного обучения. А также определение потенциальных проблем и перспектив в области верификации подписи с использованием нейросетевых подходов, чтобы предоставить рекомендации для дальнейших исследований и разработок в этой сфере.

Основная часть. Ранние методы верификации рукописной подписи в основном основывались на экспертной оценке. Судебные эксперты-криминалисты изучали отличительные черты подписи, такие как форма букв, сложность линий, скорость и давление письма, а также наклон и размеры символов. В этих методах были включены статистические подходы и методы сравнения черт рукописи. Однако эти методы имеют ряд ограничений, таких как высокая степень субъективности, низкая масштабируемость и невысокая точность.

С развитием технологий и распространением компьютеров, внимание исследователей переключилось на автоматические методы верификации подписи, основанные на машинном обучении. Эти подходы используют алгоритмы, основанные на большом количестве образцов, для анализа и сравнения черт подписей. В первых исследованиях были применены различные методы машинного обучения, такие как k-ближайших соседей (k-NN), опорные вектора (SVM) и деревья решений [1].

В последние годы нейронные сети зарекомендовали себя как мощный инструмент для распознавания образов. Это привело к развитию различных нейросетевых подходов к верификации собственноручной подписи, включая следующие:

– сверточные нейронные сети (CNN);
– рекуррентные нейронные сети (RNN);
– сети с долгой краткосрочной памятью (LSTM);
– сети глубокого обучения с подкреплением (DRL);
– трансформеры (Transformer Neural Networks).

Сверточные нейронные сети (CNN) являются типом глубоких нейронных сетей, специализирующихся на анализе визуальных образов. Они состоят из последовательности сверточных, пулинговых и полносвязных слоев (таблица 1), позволяющих автоматически извлекать иерархические признаки из изображений [2].

Таблица 1 – Виды слоев, используемых в сверточных нейронных сетях

Слои	Описание
Входной слой	Принимает изображение подписи
Сверточный слой	Применяет фильтры для извлечения локальных признаков
Пулинговый слой	Уменьшает размерность данных, сохраняя важные признаки

Полносвязный слой	Производит классификацию извлеченных признаков
Выходной слой	Возвращает вероятность того, что подпись является подлинной

CNN хорошо справляются с распознаванием различных стилей подписей и устойчивы к масштабированию, вращению и другим преобразованиям изображений.

На рисунке 1 отображен пример модели сверточной нейронной сети для распознавания и верификации собственноручной подписи.

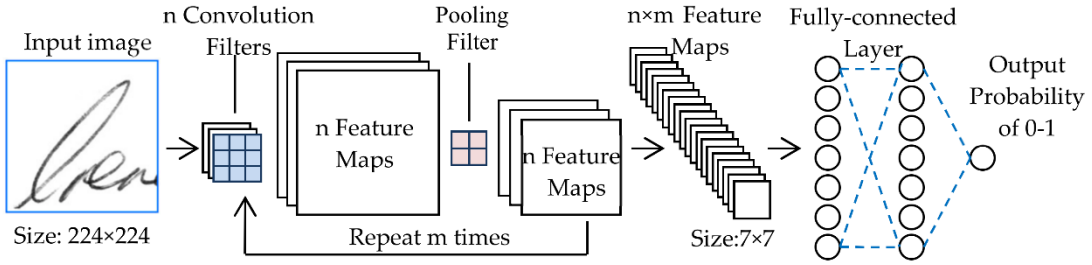

Рисунок 1 – Пример модели сверточной нейронной сети для верификации собственноручной подписи

На вход подается изображение подписи фиксированного размера. На следующем этапе входное изображение обрабатывается с помощью набора сверточных фильтров (ядер). Сверточные фильтры (convolutional filters) скользят по входным данным, применяя операцию свертки. Результаты свертки формируют карты признаков (feature maps). Далее пулинговый слой (pooling layer) уменьшает размерность карт признаков, сохраняя при этом важные признаки. Это делается путем применения агрегирующей операции, такой как максимальное или среднее значение, к непересекающимся областям карты признаков. Пулинг уменьшает вычислительную сложность модели и делает ее менее чувствительной к незначительным изменениям входных данных. После нескольких сверточных и пулинговых слоев, полученные карты признаков передаются в один или несколько полносвязных слоев, которые представляют собой традиционные многослойные персептроны. Выходной слой данной модели содержит один нейрон, определяющий, является ли представленная на изображении подпись подлинной или поддельной.

Рекуррентные нейронные сети (RNN) разработаны для работы с последовательными данными, такими как временные ряды или текст. В контексте верификации подписи RNN обрабатывают данные о траектории движения пера, такие как координаты, скорость и давление [3]. Данный тип сети хорошо учитывает временные зависимости и может обнаруживать подделки, сделанные с использованием различных техник мошенничества. Виды слоев, используемых в рекуррентных нейронных сетях, представлены в таблице 2.

Таблица 2 – Виды слоев, используемых в рекуррентных нейронных сетях

Слои	**Описание**
Входной слой	Принимает изображение подписи
Рекуррентный слой	Обрабатывает последовательность, сохраняя информацию о предыдущих состояниях
Выходной слой	Возвращает вероятность того, что подпись является подлинной

Сети с долгой краткосрочной памятью (LSTM) являются разновидностью рекуррентных нейронных сетей, которые специально разработаны для обработки долгосрочных зависимостей в данных. Они состоят из специальных ячеек памяти, которые позволяют им сохранять и обновлять информацию на длительных промежутках времени. LSTM особенно подходят для анализа сложных и изменчивых характеристик рукописной подписи, таких как скорость и давление.

Сети глубокого обучения с подкреплением (DRL) используют стратегию обучения, основанную на опыте, для оптимизации процесса принятия решений. В контексте верификации подписи DRL может быть использован для адаптации и улучшения процесса извлечения признаков и классификации. Данный тип сети может адаптироваться к новым и изменяющимся обстоятельствам, что делает его потенциально полезным для обнаружения современных подделок и мошенничества.

Трансформеры (Transformer Neural Networks) представляют собой относительно новый класс нейросетевых моделей, основанных на механизме внимания. Они позволяют моделям уделять больше внимания определенным частям данных, что может улучшить качество верификации подписи. Трансформеры были успешно применены в задачах обработки естественного языка и начинают использоваться в области верификации подписей [4]. Варианты архитектур трансформеров, такие как BERT и GPT, могут быть адаптированы для работы с изображениями и последовательностями данных, связанными с рукописными подписями.

Схема разработанной системы верификации собственноручной подписи представлена на рисунке 2.

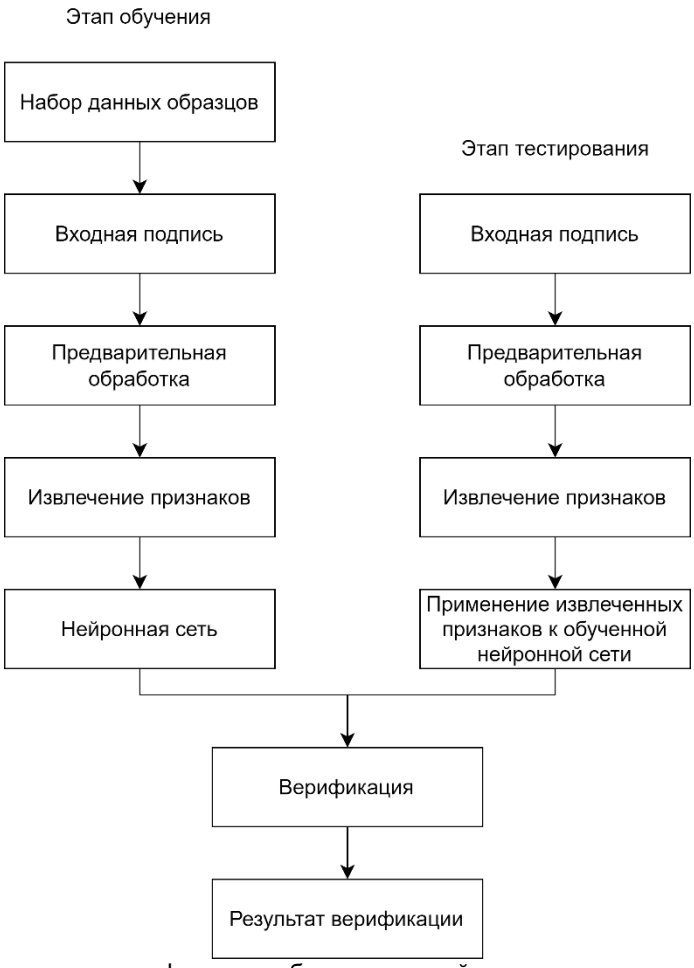

Рисунок 2 – Схема системы верификации собственноручной подписи с использованием нейронной сети

Для оценки эффективности нейросетевых и классических методов машинного обучения в задаче верификации рукописных подписей можно рассмотреть следующие критерии сравнения: точность и скорость.

Точность является одним из наиболее важных показателей эффективности алгоритма верификации подписей. Она определяет процент правильно классифицированных подписей (как подлинных, так и поддельных) от общего числа подписей в тестовом наборе данных. В целом, нейросетевые методы демонстрируют более высокую точность в задаче верификации рукописных подписей по сравнению с классическими методами машинного обучения. Это связано с тем, что нейросетевые методы могут автоматически извлекать иерархические признаки и учитывать сложные зависимости в данных, что делает их более мощными и адаптивными к различным стилям подписей и видам подделок.

Скорость относится к времени, необходимому для обработки и верификации подписи. В реальных условиях, особенно в системах, где требуется быстрое принятие решений, скорость является критическим фактором. Скорость может быть измерена как время обучения модели и время инференции (предсказания) для каждой подписи. В плане скорости обучения и инференции, классические методы машинного обучения, такие как SVM, деревья решений и k-NN, могут быть быстрее нейросетевых подходов, особенно на небольших наборах данных. Однако с увеличением объема данных и сложности задачи, нейросетевые методы могут обеспечивать более быстрое обучение и предсказание благодаря их распределенной и параллельной архитектуре.

Существующие подходы к верификации рукописных подписей, включая нейросетевые методы, имеют ряд недостатков, которые могут влиять на их эффективность и применимость в реальных условиях, а именно: требование больших объемов данных, вычислительная сложность и устойчивость к атакам и подделкам.

Перспективными направлениями для развития новых методов верификации собственноручной подписи можно рассмотреть федеративное, активное и однокадровое типы обучения.

Федеративное обучение (federated learning) может помочь решить проблемы сбора данных и защиты конфиденциальности пользователей. Оно позволяет обучать нейросетевые модели на данных, которые распределены между различными устройствами и организациями, не требуя централизованного хранения данных [5].

Активное обучение (active learning) может помочь решить проблемы с разметкой больших объемов данных. При активном обучении модель сама определяет, какие примеры наиболее полезны для обучения, и запрашивает разметку только для них, что сокращает время и стоимость разметки данных.

Однокадровое обучение (one-shot learning) может быть полезным для обучения моделей верификации подписи, когда доступно ограниченное количество образцов подписей для каждого пользователя [6]. Однокадровое обучение фокусируется на быстром адаптировании модели к новым данным с минимальным количеством примеров, что может обеспечить эффективное обучение даже при небольших наборах данных.

Для улучшения общей надежности и безопасности системы аутентификации можно интегрировать верификацию собственноручной подписи с другими биометрическими системами, такими как распознавание отпечатков пальцев, распознавание лиц и распознавание голоса. Многофакторная аутентификация может быть использована для усиления защиты и повышения устойчивости к атакам и подделкам.

Заключение. В данном исследовании был проведен обзор существующих подходов к верификации собственноручной подписи, с акцентом на нейросетевых методах, таких как сверточные нейронные сети, рекуррентные нейронные сети, сети с долгой краткосрочной памятью, сети глубокого обучения с подкреплением и трансформеры. Эти методы были сравнены с классическими методами машинного обучения по критериям, таким как точность, скорость, устойчивость к атакам и подделкам. Также были рассмотрены их преимущества и недостатки.

Для дальнейших исследований и разработок в области верификации собственноручной подписи рекомендуется:

– исследовать и разрабатывать новые архитектуры нейросетей и методы обучения;

– рассмотреть применение федеративного, активного и однокадрового обучения для решения проблем сбора и разметки данных, а также для улучшения эффективности обучения моделей;

– исследовать возможности интеграции верификации собственноручной подписи с другими биометрическими системами, чтобы создать многофакторные системы аутентификации с повышенной безопасностью и надежностью.

В целом, исследование нейросетевых методов верификации собственноручной подписи является важным шагом на пути к созданию более безопасных, надежных и удобных систем аутентификации, которые могут быть широко использованы в различных отраслях и сферах деятельности, таких как банковское дело, юриспруденция и электронная коммерция.

Список использованных источников:

1. Impedovo, D. Automatic signature verification: The state of the art / D. Impedovo, & G. Pirlo // IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2008. – P. 609-635.

2. Graves, A. Learning features for offline handwritten signature verification using deep convolutional neural networks / L.G. Hafemann, R. Sabourin, L.S. Oliveira // Pattern Recognition, 2017. – P. 163-176.

3. Graves, A. Offline handwriting recognition with multidimensional recurrent neural networks / A. Graves, J. Schmidhuber // Advances in Neural Information Processing Systems, 2009. – P. 545-552.

4. Yousef, M. Handwritten Text Recognition using Transformers / M. Yousef, M.M. Abdelsamea, G.A. Gnecco // Proceedings of the 29th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning (ESANN), 2021. – P. 371-376.

5. McMahan, H.B. Communication-Efficient Learning of Deep Networks from Decentralized Data / H.B. McMahan [at el.] // Proceedings of the 25th International Conference on Artificial Intelligence and Statistics (AISTATS), 2017. – P. 371-376.

6. Vinyals, O. Matching networks for one shot learning / O. Vinyals [at el.] // Advances in neural information processing systems, 2016. – P. 3630-3638.

UDC 004.932.2

DEVELOPMENT AND EVALUATION OF NEURAL NETWORK METHODS FOR HANDWRITTEN SIGNATURE VERIFICATION

Miskevich P.L., Petravets U.N., Ralovets A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Volorova N.A. – PhD in Engineering, Associate Professor

Annotation. Handwritten signature is a unique biometric feature, widely used for verifying identity and consent for various operations. With the rise of cyber threats and signature forgery, there is a need for reliable and efficient signature verification systems. In this article, the development of neural network methods for handwritten signature verification is discussed, existing approaches are analyzed, challenges are identified, and possible prospects are considered.

Keywords. Signature verification, neural networks, biometric authentication, cyber treats, forgery detection.