

С.В. ЗАТЕЕВ, Е.Ю. КОСТЮЧЕНКО, А.А. ШЕЛУПАНОВ
**СРАВНИТЕЛЬНЫЙ АНАЛИЗ ПОДХОДОВ
К ПРОЕКТИРОВАНИЮ АРХИТЕКТУРЫ СВЕРТОЧНЫХ
НЕЙРОННЫХ СЕТЕЙ ДЛЯ АНАЛИЗА КЛАВИАТУРНОГО
ПОЧЕРКА**

Затеев С.В., Костюченко Е.Ю., Шелупанов А.А. Сравнительный анализ подходов к проектированию архитектуры сверточных нейронных сетей для анализа клавиатурного почерка.

Аннотация. В условиях повсеместной цифровизации и учащения случаев компрометации конфиденциальной информации актуальность разработки надежных систем аутентификации, выступающих в качестве первоочередного защитного рубежа, становится критически важной. Перспективным решением проблем, связанных с утратой, кражей или несанкционированным использованием статических идентификаторов, представляются биометрические системы поведенческого типа. В частности, методы, основанные на анализе клавиатурного почерка (динамики работы с клавиатурой), позволяют осуществлять непрерывную и скрытую аутентификацию пользователя на протяжении всего сеанса работы, анализируя его уникальные и трудно подделываемые поведенческие паттерны. Данное направление характеризуется сочетанием высокого уровня безопасности с относительно умеренными затратами на внедрение и высоким удобством для конечного пользователя. Целью настоящего исследования является проведение сравнительного анализа различных подходов к проектированию и построению архитектур сверточных нейронных сетей, оптимизированных для обработки разреженных данных, описывающих динамику нажатий клавиш. В ходе экспериментальной работы было установлено, что сверточные нейронные сети демонстрируют исключительно высокую точность верификации, достигающую 99%, несмотря на то, что входные данные, сформированные в результате предобработки, обладают сильной разреженностью. Наилучшие результаты в рамках исследования были достигнуты при использовании архитектуры, основанной на механизме разделенной свертки, которая показала свою эффективность для работы с указанным специфическим типом данных.

Ключевые слова: аутентификация, поведенческая биометрия, клавиатурный почерк, разреженные данные, сверточные нейронные сети.

1. Введение. Современное общество характеризуется глубокой интеграцией информационных систем в различные сферы человеческой деятельности. В цифровой среде хранятся значительные массивы данных, включая персональную информацию и сведения, составляющие коммерческую тайну. Как следствие, задача обеспечения информационной безопасности, подразумевающая комплекс мер по защите данных от несанкционированного вмешательства, стала одним из ключевых направлений в области информационных технологий. Ее актуальность постоянно поддерживается прогрессом в методах кибератак, что требует адекватного и опережающего развития защитных механизмов.

В данном контексте системы аутентификации, выполняющие роль первоначального барьера на пути к информационным ресурсам, становятся критически важными. Их фундаментальная задача – верификация подлинности субъекта путем сопоставления предъявленных характеристик с эталонными образцами, зарегистрированными в системе.

Существующие методы аутентификации традиционно классифицируются по типу используемого идентификатора:

1. Знание: использование паролей или PIN-кодов. Несмотря на простоту реализации, этот подход уязвим к краже, фишингу и brute-force атакам, что ставит под сомнение его надежность.

2. Владение: применение физических носителей, таких как токены или карты доступа. Главные недостатки включают риск утери или кражи идентификатора, а также необходимость в дополнительной инфраструктуре, что повышает сложность и стоимость системы.

3. Биометрические данные: использование уникальных биологических или поведенческих характеристик. Биометрию принято разделять на физиологическую и поведенческую. К физиологической относят отпечатки пальцев, радужную оболочку глаза и другие неизменяемые признаки. Такие данные надежны, но статическая природа делает их уязвимыми для компрометации и воспроизведения. Поведенческая биометрия включает голос, походку и динамику работы с клавиатурой. Эти характеристики сложнее подделать благодаря отсутствию статичного шаблона. Однако их изменчивость под влиянием состояния пользователя может снижать стабильность и надежность.

Ключевой недостаток традиционных систем статической аутентификации – их неспособность обнаружить факт смены пользователя после первоначального входа. Биометрические системы, основанные на поведенческих характеристиках, предлагают решение этой проблемы, обеспечивая постоянный мониторинг.

Особый интерес в этом направлении представляют системы, анализирующие клавиатурный почерк – поведенческий биометрический идентификатор, основанный на уникальных паттернах взаимодействия пользователя с клавиатурой. Данный подход обладает рядом значительных преимуществ:

- ненавязчивость и прозрачность: не требуют дополнительного оборудования, используя стандартные устройства ввода;
- непрерывность: позволяет осуществлять верификацию на протяжении всего сеанса работы;

– многофакторность: анализирует комплекс параметров, таких как ритм печати, длительность нажатий и интервалы между ними.

Современные стандарты в области информационной безопасности признают клавиатурный почерк в качестве уникальной и перспективной характеристики для построения динамических систем защиты. В то время как аутентификация по статическим парольным фразам является хорошо изученной областью [1, 2, 3], исследования в сфере непрерывной поведенческой биометрии, в частности анализа клавиатурного почерка, находятся на стадии активного развития [3, 4]. Это направление представляется чрезвычайно перспективным, поскольку позволяет достичь высокого уровня безопасности, сочетая его с удобством для пользователя и экономической эффективностью внедрения.

Как показывает практика, в силу специфики формата данных, необходимого для обработки сверточными нейронными сетями, в итоговый набор данных попадает множество признаков, не обладающих должным уровнем информативности. Полученные матрицы характеризуются высокой степенью разреженности, что может приводить к снижению точности распознавания пользователей.

Таким образом, необходимо провести анализ эффективности использования сверточных нейронных сетей для решения задачи аутентификации по фактору клавиатурного почерка, построив архитектуру, которая бы грамотно обрабатывала такие разреженные данные. Кроме того, необходимо определиться с параметрами формирования многоканальных матриц, обеспечивающими лучшее качество работы модели сверточной нейронной сети.

2. Набор данных. Исходный набор данных, описывающий поток событий, фиксируемых при взаимодействии пользователя с клавиатурой, разбивается на интервалы, в соответствии с принципами, описанными в работах [5 – 9]. Интервалы формируются как пересекающиеся окна, содержащие фиксированное количество событий. В качестве параметров используются те, которые показали лучший результат в работах [5, 6]: количество событий в окне – 2000, пересечение – 50% от длины окна. На каждом интервале производится расчет признаков биграмм как в работе [10], однако в данном случае биграммы состояются из наиболее часто встречающихся клавиш [5]. Частоты употребления считаются по всей имеющейся выборке. Также в данной работе кроме среднего выборочного значения признака для каждого интервала используется расширенный набор статистических характеристик: среднее квадратичное отклонение, коэффициенты асимметрии и эксцесса. Кроме того, в данной работе

используются лишь три из пяти каналов, употребляемых в работе [10]. Так как продолжительность удержания отдельной клавиши и любой из 4-х признаков биграмм могут быть рассчитаны на основании оставшихся 3-х признаков набора биграмм. Рассчитанные признаки собираются в многоканальную матрицу по следующему принципу: измерения каждого канала – первая и вторая клавиши, составляющие биграмму, каналы – признаки биграмм. Признаки биграмм выделяются на основании принципов, изложенных в работах [5, 8, 11]. Размер матрицы определяется количеством используемых клавиш, чем больше размер, тем больше информации помещает в себя матрица, но увеличивается время ее обработки. Кроме того, чем реже используются клавиши, тем реже используются биграммы, содержащие их, а значит, появляется риск возникновения большого количества пустых значений в матрице, что может негативно сказаться на качестве работы модели. В данной работе осуществляется следующий принцип подбора значений: исследуются от 5 до 50 (с шагом 5) наиболее часто встречающихся клавиш.

Формирование многоканальной матрицы иллюстрирует рисунок 1. На основе каждого интервала выделяются 4 сегмента матрицы, каждый из которых заполняется значениями одной статистической характеристики (среднее выборочное в рамках интервала, среднее квадратичное отклонение, коэффициенты асимметрии и эксцесса). Каждый сегмент представляет собой матрицу размером $K \times K$ (K – количество наиболее часто встречающихся клавиш), содержащую 3 канала – по одному на каждый признак биграммы. Для набора данных, содержащих только средние значения, используется только один из сегментов (трехканальная матрица размера $K \times K$). Для набора с полным набором статистических характеристик проводится конкатенация четырех сегментов, которая укладывает их в блок 2×2 , как показано на рисунке 1, и увеличивает пространственный размер матрицы вдвое по каждой оси. При этом соответствующие каналы каждого сегмента конкатенируются между собой. В результате получается трехканальная матрица размером $2K \times 2K$.

Итоговый набор данных представляет собой совокупность интервалов из исходного набора данных, преобразованных к формату многоканальных матриц. На рисунке 2 представлено распределение интервалов по пользователям. Суммарно выделено 11 287 интервалов. Как можно заметить на рисунке, в данных нет очевидного дисбаланса классов. Один класс превосходит в 2 раза по количеству образцов средний уровень по набору данных, но это превосходство

нивелируется количеством классов. Превосходящий класс не занимает даже 10% от всего набора.

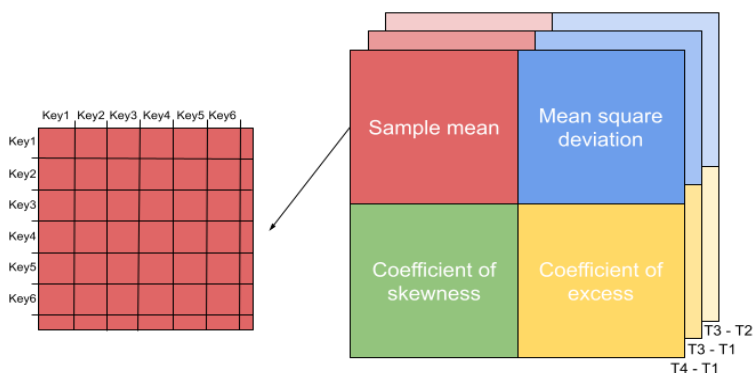


Рис. 1. Образование итоговой многоканальной матрицы

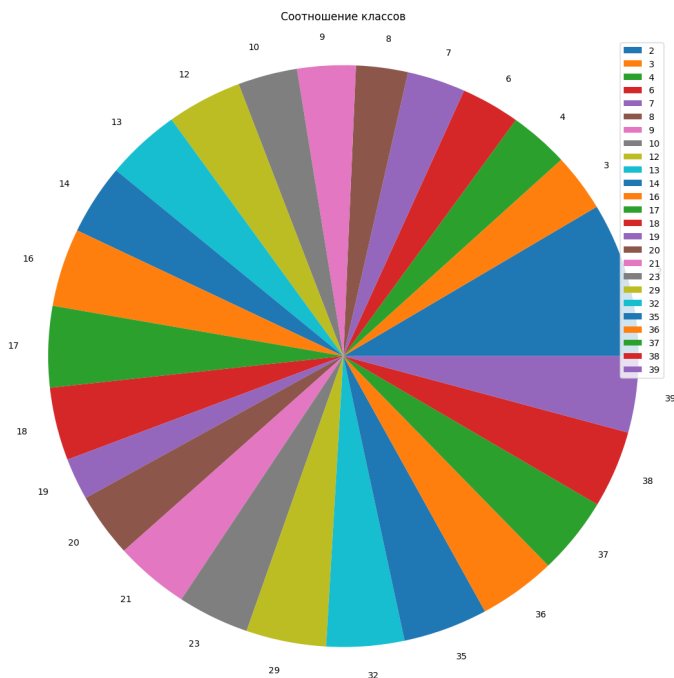


Рис. 2. Соотношение классов в итоговом наборе данных

3. Архитектуры модели

3.1. Классическая сверточная нейронная сеть. Сверточная нейронная сеть (CNN) – это специализированная архитектура глубокого обучения, разработанная для обработки данных с сеточной структурой, таких как изображения, временные ряды и пространственные данные. Основная идея CNN заключается в автоматическом извлечении иерархических признаков с помощью операций свертки и пулинга, что позволяет эффективно учитывать локальные зависимости в данных.

Архитектура используемой модели представлена на рисунке 3. Она состоит из N блоков свертки, каждый из которых состоит из двух сверток 3×3 и максимального пулинга 2×2 , количество каналов в каждом блоке прямо пропорционально порядковому номеру блока и кратно 32. Последний блок состоит из двух полносвязных слоев классификатора с 200 нейронами в первом полносвязном слое и 25 – во втором.

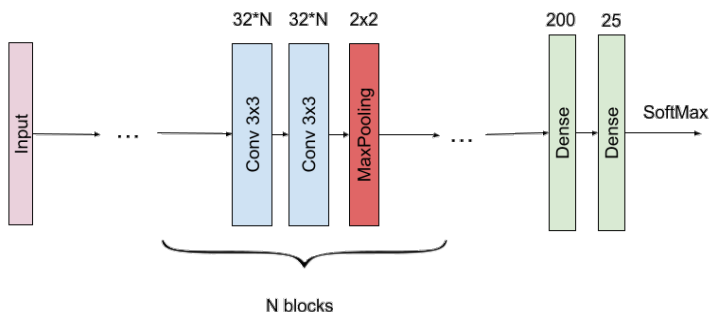


Рис. 3. Архитектура сверточной нейронной сети

Такая архитектура обусловлена желанием использовать максимум возможностей сверточных нейронных сетей для оценки информативности признаков, выделенных при помощи разных подходов. Размерность матриц в экспериментах варьируется от 5×5 (только средние значения и 5 наиболее часто употребляемых клавиш) до 100×100 (полный набор статистических характеристик, удваивающий размер матрицы, и 50 наиболее часто употребляемых клавиш). Архитектура, достаточно глубокая для обработки матрицы 100×100 , не сможет корректно свернуть матрицу 5×5 . И наоборот: сеть, оптимальная для маленьких матриц, окажется недостаточно глубокой для анализа больших. Из этих соображений архитектура подбирает глубину сети в зависимости от размерности многоканальной матрицы.

Так как главное ограничение, вытекающее из маленького размера матрицы, является невозможность свернуть ее определенное количество раз при помощи пулинга, уменьшающего размерность в 2 раза, то и максимальная глубина сети рассчитывается как количество раз, которое размерность матрицы можно сократить вдвое, не превратив ее в единицу (1).

$$MaxDepth = \lfloor \log_2 MatrixDimension \rfloor - 1, \quad (1)$$

где $MatrixDimension$ – количество строк в квадратной матрице.

3.2. Дилатированная сверточная нейронная сеть.

Дилатированная сверточная нейронная сеть (DCNN) – это разновидность сверточной нейронной сети, использующая дилатированную свертку – операцию, применяемую к входным данным с пропуском элементов между ядром согласно параметру, называемому коэффициент дилатации. Коэффициент дилатации определяет, насколько растягивается ядро свертки. [12]

Архитектура используемой модели почти полностью идентична предыдущей и представлена на рисунке 4. Она состоит из N блоков свертки, каждый из которых состоит из двух сверток 3×3 и максимального пулинга 2×2 , количество каналов в каждом блоке прямо пропорционально порядковому номеру блока и кратно 32. Отличие от предыдущей архитектуры заключается в том, что первая из сверток в каждом блоке является дилатированной (разреженной). Последний блок состоит из двух полносвязных слоев классификатора с 200 нейронами в первом полносвязном слое и 25 – во втором. Расчет глубины осуществляется способом, обозначенным в (1).

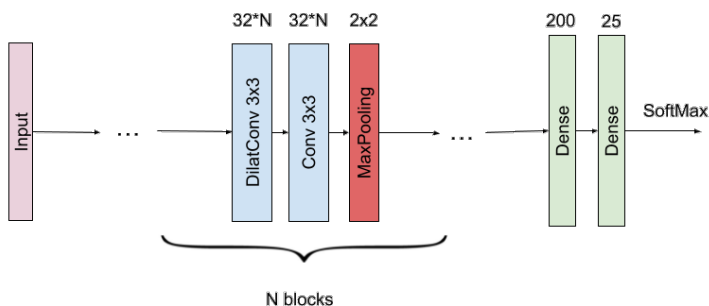


Рис. 4. Архитектура дилатированной сверточной сети

Логика использования такой архитектуры в рамках данной задачи предельно проста. В анализе изображений при помощи нейронных сетей свертка выполняет одну важную функцию – она вычисляет контекст пикселя изображения. Таким образом, при анализе учитываются не только значения того или иного пикселя, но и их взаимное расположение. Очевидно, что в задачах распознавания объектов, сегментации и т.д. наиважнейшие зависимости будут касаться ближайших пикселей (если текущий пиксель принадлежит искомому объекту или определенной закономерности, то и ближайшие ему пиксели с большой вероятностью будут принадлежать тому же объекту или той же закономерности). Однако, это не совсем характерно для текущей задачи. Строго говоря, собранные многоканальные матрицы кроме формы имеют мало общего с действительными изображениями, так как пространственные зависимости между пикселями в данном контексте носят абстрактный характер, в отличие от геометрических зависимостей в реальных изображениях. Размерности каналов матрицы соответствуют наиболее часто встречающимся клавишам. Но эти клавиши далеко не всегда входят в состав наиболее часто встречающихся биграмм. Как следствие, плотность последних в итоговых матрицах невелика, что и подтверждается высокой степенью разреженности данных. Поэтому важные зависимости далеко не всегда находятся между соседними пикселями и могут быть распределены по всей матрице. В связи с этим имеет смысл использовать разреженное ядро свертки для поиска более удаленных друг от друга зависимостей.

3.3. Сверточная нейронная сеть с комбинированной архитектурой. Предположительно, дилатированная свертка в чистом виде может быть неоптимальна для данной задачи, так как важные зависимости могут существовать как на локальном, так и на глобальном уровне. Поэтому была предложена комбинированная архитектура, объединяющая классическую и дилатированную свертки. Она представлена на рисунке 5.

Архитектура состоит из N блоков свертки, каждый из которых имеет следующий состав: распараллеленные слои классической свертки 3×3 и дилатированной свертки 3×3 с количеством каналов в каждом слое прямо пропорционально порядковому номеру блока и кратно 16, результаты обработки этими слоями конкатенируются и поступают на блок классической свертки 3×3 с количеством выходных каналов, прямо пропорциональным порядковому номеру блока и кратно 32. Последний блок состоит из двух полносвязных слоев классификатора с 200

нейронами в первом полносвязном слое и 25 – во втором. Расчет глубины осуществляется способом, обозначенным в (1).

Логика использования такой архитектуры следующий. Если важные зависимости могут существовать как на локальном, так и на глобальном уровне, значит, имеется больше логики в поиске зависимостей в признаках, расположенных в соседних ячейках матрицы. Однако, если в использовании дилатированной свертки есть смысл, то один из параллельных слоев будет анализировать соседние ячейки, а другой – расположенные на расстоянии одной ячейки друг от друга. Тем самым происходит одновременно анализ на большем пространстве, как при дилатированной свертке, но не теряются зависимости на меньшем пространстве.

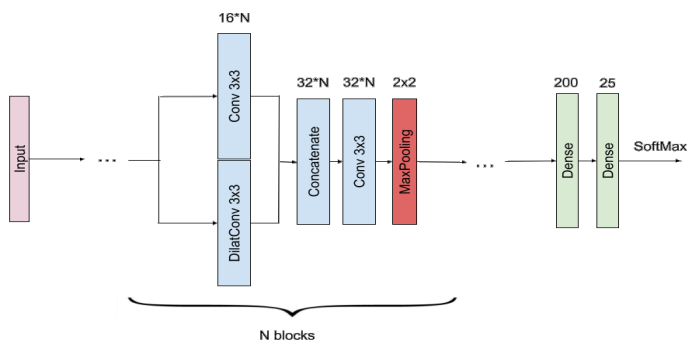


Рис. 5. Архитектура комбинированной сверточной сети

3.4. Сверточная нейронная сеть с увеличенным размером ядра.

Дилатированная свертка нацелена на поиск удаленных зависимостей, однако не исключено, что для данной задачи может потребоваться анализ более широкого локального контекста, чем обеспечивает ядро 3×3 . Альтернативным способом расширения анализируемого контекста является увеличение размера ядра свертки. Архитектура с ядром 5×5 представлена на рисунке 6. Она состоит из N блоков свертки, каждый из которых состоит из двух последовательных сверток 5×5 , 3×3 и максимального пулинга 2×2 , количество каналов в каждом блоке прямо пропорционально порядковому номеру блока и кратно 32. Последний блок состоит из двух полносвязных слоев классификатора с 200 нейронами в первом полносвязном слое и 25 – во втором. Расчет глубины осуществляется способом, обозначенным в (1).

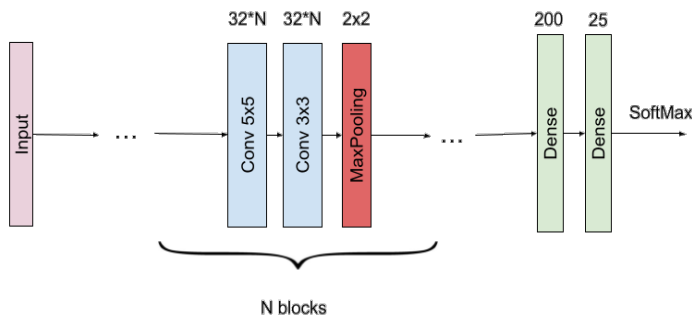


Рис. 6. Архитектура сверточной сети с увеличенным ядром

3.5. Поканальная разделенная сверточная нейронная сеть.

Поканальная разделенная сверточная нейронная сеть (Depthwise Separable Convolution) – это разновидность сверточной нейронной сети, использующая разделенную свертку – операцию, разделяющую стандартную свертку на два этапа: depthwise-свертку, где каждый входной канал обрабатывается отдельным фильтром, и pointwise-свертку (1x1), которая комбинирует результаты через линейную проекцию. Такой подход значительно сокращает количество параметров и вычислительную сложность при сохранении способности извлекать пространственные и межканальные зависимости [13].

Архитектура используемой модели почти полностью идентична классической и представлена на рисунке 7. Она состоит из N блоков свертки, каждый из которых состоит из двух сверток 3x3 и максимального пулинга 2x2, количество каналов в каждом блоке прямо пропорционально порядковому номеру блока и кратно 32. Отличие от предыдущей архитектуры заключается в том, что обе свертки в каждом блоке являются разделенными. Последний блок состоит из двух полносвязных слоев классификатора с 200 нейронами в первом полносвязном слое и 25 – во втором. Расчет глубины осуществляется способом, обозначенным в (1).

Логика использования такой архитектуры в рамках данной задачи заключается в следующем. Так как такие слои разделяют пространственную и межканальную свертки, предоставляется возможность обнаружить зависимости между признаками на различных каналах (т.е. различных признаков одних и тех же биграмм). Также pointwise-свертка позволяет сконцентрироваться не только на контексте признаков, но и на значениях самих признаков. Кроме того, такие архитектуры эффективны на малых данных, что соответствует текущей задаче (всего 11 тысяч образцов).

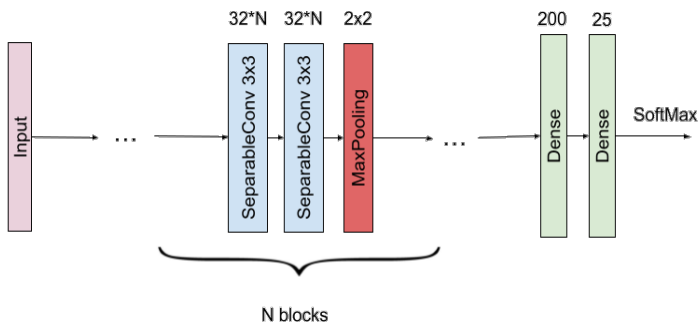


Рис. 7. Архитектура разделенной сверточной сети

3.6. Сверточная нейронная сеть с маскированием. В данной задаче маска – это матрица той же размерности, что и некоторый набор признаков внутри сверточной нейронной сети. Прежде чем этот набор признаков будет обработан очередной сверткой, рассчитывается маска, содержащая нули на тех же позициях, где содержат нули исходные данные, и единицы на остальных позициях. После обработки набора признаков сверткой каждый канал результата этой обработки поэлементно умножается на маску. Такой подход позволяет напрямую указать нейронной сети на каких позициях в наборе признаков находятся реальные данные, а на каких – пустые ячейки.

Архитектура используемой модели почти полностью идентична классической и представлена на рисунке 8. Она состоит из N блоков свертки, каждый из которых состоит из двух сверток 3×3 и максимального пулинга 2×2 , количество каналов в каждом блоке прямо пропорционально порядковому номеру блока и кратно 32. Отличие от предыдущей архитектуры заключается в том, что в начале каждого блока рассчитывается маска для набора признаков, а после каждой свертки осуществляется умножение результата обработки на эту маску. Последний блок состоит из двух полносвязных слоев классификатора с 200 нейронами в первом полносвязном слое и 25 – во втором. Расчет глубины осуществляется способом, обозначенным в (1).

Маскирование применяется для явного указания значимых областей в разреженных данных, предотвращая распространение нулевых значений через слои нейронной сети. В предлагаемом подходе бинарная маска инициализируется на входном слое каждого блока. На каждом сверточном слое маска поэлементно умножается на выходные карты признаков, эффективно обнуляя области без исходной информации. Это позволяет сети фокусироваться только

на релевантных паттернах и предотвращает обучение на артефактах, возникающих из-за разреженности данных. Реализованный механизм сквозного маскирования существенно улучшает устойчивость модели к зашумленным и неполным данным, что критически важно для задач биометрической идентификации по динамике нажатия клавиш.

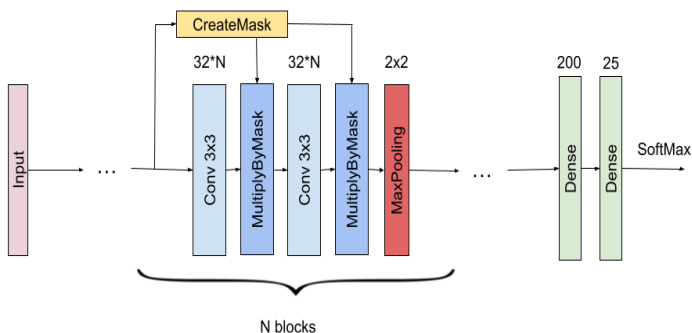


Рис. 8. Архитектура маскированной сверточной сети

4. Процедура разбиения данных и оценки устойчивости полученных результатов. Исходный набор данных изначально разбит на сессии для каждого пользователя. Ввиду ограниченного количества сессий и их существенно различной длины, разбиение на обучающую, валидационную и тестовую выборки выполнялось вручную с соблюдением следующих условий:

- для каждого пользователя выборки формировались из целых сессий, при этом все записи одной сессии относились строго к одной выборке (таким образом, исключалось попадание записей из одной сессии в разные выборки, загрязнение тестовой выборки не происходит);

- целевое соотношение объемов записей для каждого пользователя составляло примерно 80 % (обучающая), 10 % (валидационная) и 10 % (тестовая);

- на полученном фиксированном разбиении для каждой из рассматриваемых моделей проводилось 5 независимых запусков обучения, результатом модели считалось выборочное среднее по этим пяти запускам.

На основе указанной процедуры для каждой архитектуры выбиралась одна лучшая модель (по метрике на тестовой выборке).

Для оценки устойчивости полученных результатов и построения доверительных интервалов была применена процедура,

имитирующая множественное разбиение данных. Было сформировано 10 различных разбиений исходного набора данных на обучающую, валидационную и тестовую выборки, каждое из которых удовлетворяло тем же правилам. На каждом из 10 разбиений заново обучались все 6 моделей.

Итоговое сравнение лучших моделей разных архитектур выполнялось по выборке из 10 значений метрики с построением доверительных интервалов.

5. Результаты. Результаты оценки информативности наборов данных при помощи классической сверточной нейронной сети в виде тепловой карты представлены на рисунке 9. В таком виде можно нагляднее сравнить влияние использования статистических характеристик на качество распознавания, а также оценить целесообразность повышения глубины архитектуры для анализа более крупных матриц. На рисунке слева (Features: Mean) расположены результаты работы модели, обученной на наборе данных, использующем для выделения признаков в рамках интервала только средние значения, справа (Features: Complete) – результаты работы модели, обученной на наборе данных, использующем полный набор статистических характеристик. Тепловая карта имеет в качестве своих измерений количество используемых клавиш (Image Size) и количество блоков в нейронной сети (Network Depth).

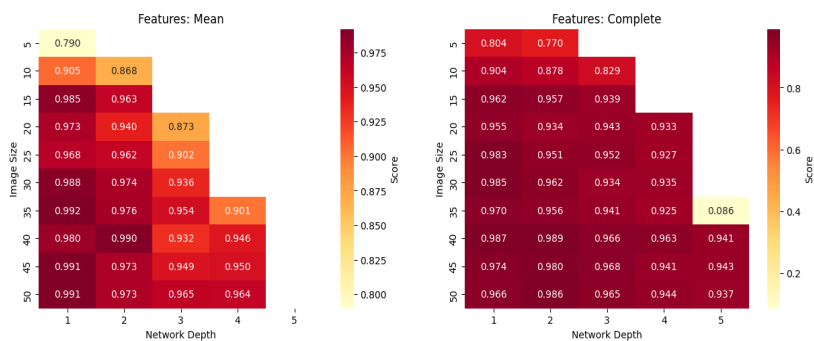


Рис. 9. Результаты оценки информативности наборов данных при помощи классической сверточной нейронной сети

Можно сделать следующие выводы:

- повышение размеров матрицы стабильно приводит к улучшению распознавания пользователей, однако увеличение размера свыше 25, это улучшение нельзя назвать качественным;

– наилучшие результаты распознавания принадлежат набору данных с использованием исключительно среднего выборочного значения, однако отличие от наилучшего результата у своего прямого аналога сложно назвать значительным (0.992 у набора со средним выборочным и 0.989 у набора с полным набором характеристик – отличие в третьем знаке), следовательно, для более точного сравнения стоит рассчитать статистическую значимость такого отличия;

– использование слишком глубоких сетей излишне: на рисунке 9 можно заметить, что лучшие результаты дают архитектуры с глубиной 1 и 2; особенно это заметно на данных, использующих исключительно среднее выборочное, даже архитектуры с глубиной 3 обрабатывают с ощутимо меньшим качеством, чем архитектуры с меньшей глубиной.

Результаты оценки информативности наборов данных при помощи дилатированной сверточной нейронной сети представлены на рисунке 10. Результаты подтверждают ранее выявленную закономерность: увеличение размера выше 25-30 не дает качественного прироста информативности.

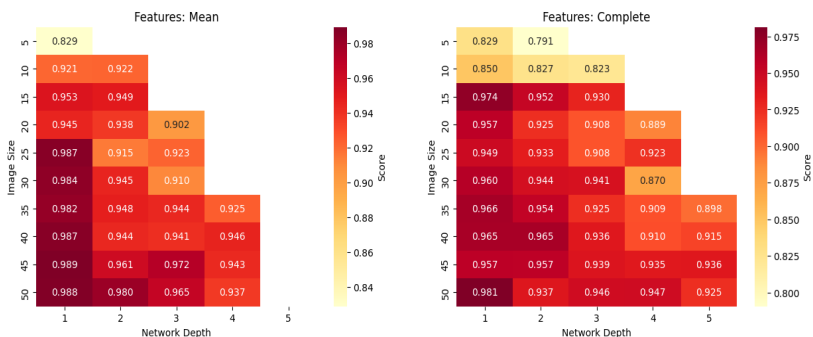


Рис. 10. Результаты оценки информативности наборов данных при помощи дилатированной сверточной нейронной сети

Выводы, следующие из результатов этого эксперимента:

– для дилатированной сверточной нейронной сети повышение размеров матрицы более 25-30, как и для классической, приводит к улучшению распознавания пользователей, однако это улучшение нельзя назвать качественным;

– наилучшие результаты распознавания принадлежат набору данных с использованием исключительно среднего выборочного значения (0.989 у набора со средним выборочным и 0.981 у набора

с полным набором характеристик – отличие в третьем знаке), однако различие сильнее, чем при использовании классической нейронной сети;

- использование слишком глубоких сетей и для дилатированных сверточных нейронных сетей излишне: модели с более глубокой архитектурой показывают результат хуже, причем разница между наилучшим и наихудшим результатами (в контексте сравнения только по глубине) выше, чем при использовании классических сверточных нейронных сетей;

- используемая архитектура дилатированных сверточных нейронных сетей уступает в качестве распознавания классическим нейронным сетям, что может говорить о том, что дилатированные свертки выгоднее было бы использовать не вместо классических, а вместе с ними.

Результаты оценки информативности наборов данных при помощи комбинированной сверточной нейронной сети представлены на рисунке 11. Как и в случае с классической CNN, увеличение размера выше 20 не дает качественного прироста информативности. Кроме того, с таким подходом архитектура с минимальной глубиной в большом количестве случаев перестает быть оптимальной.

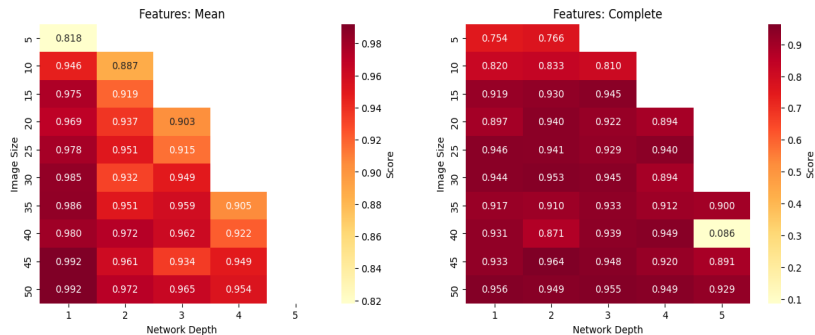


Рис. 11. Результаты оценки информативности наборов данных при помощи комбинированной сверточной нейронной сети

Результаты показывают, что:

- для комбинированной сверточной нейронной сети повышение размеров матрицы более 20 приводит к улучшению распознавания пользователей, однако это улучшение нельзя назвать качественным;
- наилучшие результаты распознавания принадлежат набору данных с использованием исключительно среднего выборочного значения (0.992 у набора со средним выборочным и 0.964 у набора

с полным набором характеристик – отличие в третьем знаке), однако различие сильнее, чем при использовании классической нейронной сети;

- использование слишком глубоких сетей и для комбинированных сверточных нейронных сетей излишне: модели с более глубокой архитектурой показывают результат хуже, причем разница между наилучшим и наихудшим результатами (в контексте сравнения только по глубине) выше, чем при использовании классических сверточных нейронных сетей;

- комбинированная архитектура сверточных нейронных сетей в среднем уступает в качестве распознавания классическим сверточным нейронным сетям, однако лучшие результаты соответствуют им.

Результаты оценки информативности наборов данных при помощи сверточной нейронной сети с увеличенной сверткой представлены на рисунке 12. Здесь также отчетливо прослеживается закономерность, отмеченная ранее.

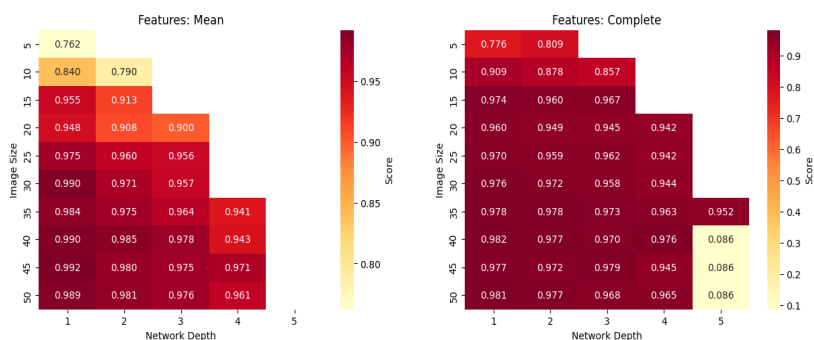


Рис. 12. Результаты оценки информативности наборов данных при помощи сверточной нейронной сети с увеличенным ядром

На рисунке 12 видно, что:

- для такой архитектуры сверточной нейронной сети повышение размеров матрицы более 25-30, как и для классической, приводит к улучшению распознавания пользователей, однако это улучшение нельзя назвать качественным;

- наилучшие результаты распознавания принадлежат набору данных с использованием исключительно среднего выборочного значения (0.992 у набора со средним выборочным и 0.981 у набора с полным набором характеристик – отличие в третьем знаке), однако различие сильнее, чем при использовании классической нейронной сети;

- использование слишком глубоких сетей излишне: модели с более глубокой архитектурой показывают результат хуже, причем

модели с глубиной в 5 блоков уже не могут адекватно обучиться, они определяют все образцы в один единственный класс;

- используемая архитектура сверточных нейронных сетей в общем не сильно уступает в качестве распознавания классическим нейронным сетям.

Результаты оценки информативности наборов данных при помощи сверточной нейронной сети представлены на рисунке 13. Качество предсказания показывает заметный рост при увеличении размеров матрицы на всем исследуемом промежутке.

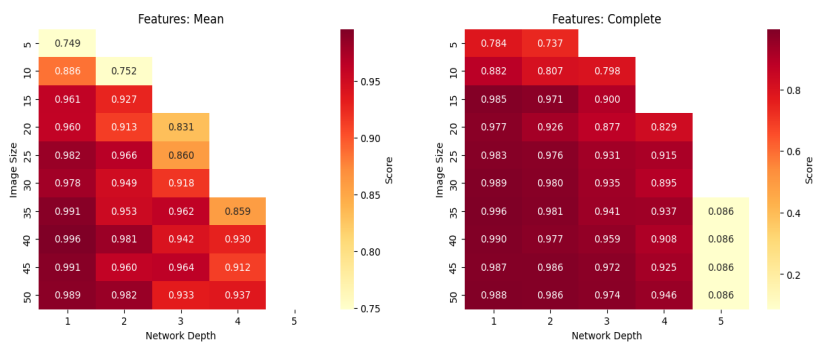


Рис. 13. Результаты оценки информативности наборов данных при помощи разделенной сверточной нейронной сети

Таким образом:

- для такой архитектуры сверточной нейронной сети повышение размеров матрицы приводит к заметному улучшению распознавания пользователей;

- наилучшие результаты распознавания принадлежат обоим наборам данных (0.996 у набора со средним выборочным и 0.996 у набора с полным набором характеристик), однако в данном случае набор данных с полным перечнем характеристик в среднем обрабатывает заметно лучше;

- использование слишком глубоких сетей излишне: модели с более глубокой архитектурой показывают результат хуже, причем все модели с глубиной в 5 блоков уже не могут адекватно обучиться, они определяют все образцы в один единственный класс;

- используемая архитектура сверточных нейронных сетей ощутимо превосходит классические нейронные сети в качестве распознавания.

Результаты оценки информативности наборов данных при помощи маскированной сверточной нейронной сети представлены

на рисунке 14. Качество предсказания показывает заметный рост на матрицах меньших размеров.

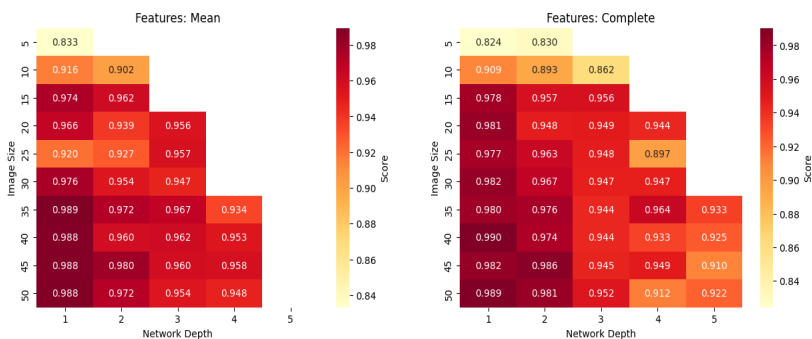


Рис. 14. Результаты оценки информативности наборов данных при помощи маскированной сверточной нейронной сети

На рисунке 14 видно, что:

- для такой архитектуры сверточной нейронной сети повышение размеров матрицы приводит к заметному улучшению распознавания пользователей;
- наилучшие результаты распознавания принадлежат набору данных с полным перечнем статистических характеристик (0.989 у набора со средним выборочным и 0.990 у набора с полным набором характеристик – отличие в третьем знаке), однако в данном случае набор данных с полным перечнем характеристик в среднем обрабатывает заметно лучше;
- использование слишком глубоких сетей излишне: модели с более глубокой архитектурой показывают результат хуже;
- используемая архитектура сверточных нейронных сетей не превосходит классические нейронные сети в качестве распознавания;
- использование масок увеличивает качество распознавания почти всех моделей, следовательно, как метод анализа разреженных данных более пригоден, чем методы с дилатированной сверткой, однако этот метод может требовать более тонкой настройки.

6. Обсуждение. Результаты оценки качества разных архитектур моделей сведены в единую таблицу, представленную на рисунке 15. В качестве значения в ячейке таблицы помещено максимальное значение среди моделей с разной глубиной, имеющих параметры обучающей выборки и архитектуру, соответствующих столбцам и строкам таблицы соответственно. В таблице отмечены лучшие результаты для каждой из архитектур.

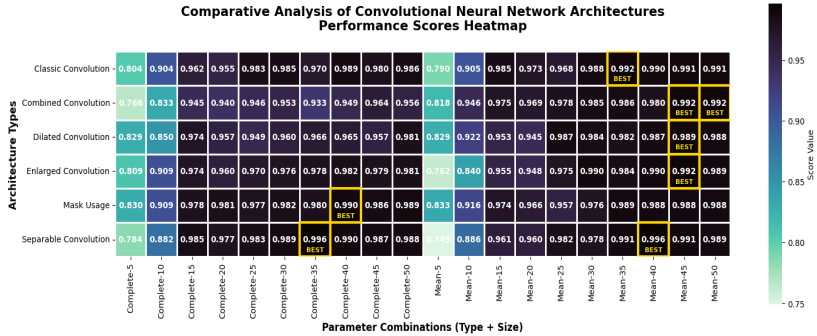


Рис. 15. Сравнение архитектур моделей

Стоит отметить несколько основных закономерностей. Увеличение размеров многоканальной матрицы путем увеличения количества анализируемых клавиш стабильно приводит к увеличению результатов вопреки выводам, сделанным при помощи оценки на основе энтропийных характеристик. Увеличение количества используемых статистических характеристик, наоборот, приводит к настолько сильной разреженности матриц, что точность предсказания на них ощутимо падает. Однако, использование определенных архитектур (архитектур с разделенной сверткой и с масками) эту проблему решает, и такие архитектуры справляются с полным набором характеристик лучше, чем с исключительно средним выборочным.

На рисунке 16 представлено сравнение наилучших представителей разных архитектур между собой с учетом доверительных интервалов, рассчитанных на основе 10 разных разбиений исходного набора данных методом, описанным в разделе 4. Для расчета доверительных интервалов была использована (2).

$$Score = MeanScore \pm t_{n-1, 0.95} * \frac{\sigma}{\sqrt{n}} \quad (2)$$

где σ – стандартное отклонение, n – количество значений в выборке (=10), t – коэффициент Стьюдента.

Как можно заметить, размеры доверительных интервалов слишком велики, чтобы можно было однозначно сравнить модели между собой. Однако, радиусы интервалов достаточно малы, чтобы сравнить эти модели с аналогами из других работ. Ключевые аналоги в области использования сверточных нейронных сетей, а также

лучшие модели, использующие иные методы машинного обучения, сведены в таблицу 1 для сравнения.

Из таблицы видно, что в среднем классическая, комбинированная и разделенная сверточная модель отрабатывают лучше, чем большинство аналогов, если верить метрике точности. Если ориентироваться по метрике EER, модели, собранные в данной работе также превосходят большинство аналогов.

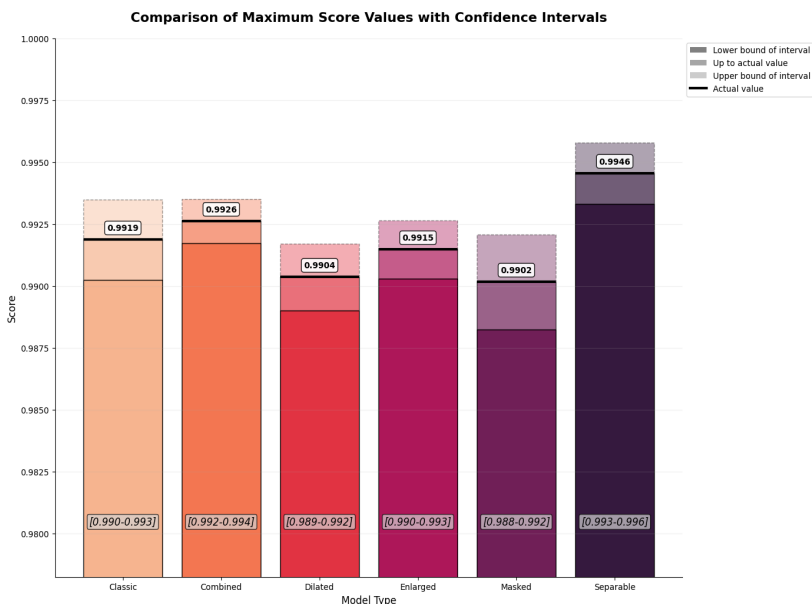


Рис. 16. Сравнение наилучших представителей разных архитектур сверточных нейронных сетей

7. Заключение. Таким образом, был проведен анализ эффективности использования сверточных нейронных сетей для решения задачи аутентификации по фактору клавиатурного почерка. По результатам анализа можно сделать следующие выводы. Классическая и комбинированная CNN показали стабильно высокие результаты, сопоставимые с лучшими аналогами. Дилатированная CNN и CNN с увеличенным ядром не превзошли классический подход, что указывает на большую важность локальных зависимостей в данных для данной задачи. Сеть с маскированием доказала свою пригодность для работы с разреженными данными, но не показала превосходства над классической CNN, требуя при этом более тонкой настройки.

Разделенная сверточная сеть продемонстрировала наилучший результат, достигнув точности 99,5% и наименьшего EER (0,2%). Ее эффективность объясняется способностью эффективно выделять зависимости между разными каналами (признаками биграмм) и высокой эффективностью на малых выборках данных.

Таблица 1. Сравнение моделей с аналогами

Источник	Метод	Точность	EER
-	Классическая сверточная нейронная сеть	99,2%	0,37%
-	Дилатированная сверточная нейронная сеть	99%	0,52%
-	Комбинированная сверточная нейронная сеть	99,3%	0,31%
-	Сверточная нейронная сеть с увеличенным ядром	99,1%	0,4%
-	Разделенная сверточная нейронная сеть	99,5%	0,2%
-	Сверточная нейронная сеть с использованием масок	99%	0,33%
[14]	XGBoost	96,39%	-
[15]	LightGBM	94,68%	-
[16]	Случайные леса	99%	-
[17]	Перцептрон	98%	-
[18]	Многослойный перцептрон	97,18%	0,02%
[19]	Статистический профиль на основе взвешенного Манхэттенского расстояния	-	5,47%
[20]	Сиамская нейронная сеть + LSTM	-	2,2%
[21]	CNN-RNN	97,77%	0,01%
[22]	Трансформер на основе CNN-GRU	96,68%	3,33%
[23]	Трансформер TypeFormer	-	3,25%
[24]	Трансформер DoubleStrokeNet	-	0,75%
[10]	Классическая сверточная нейронная сеть	92%	-
[25]	Сверточная нейронная сеть + Рекуррентная сеть	98,7%	-
[26]	Гибридная архитектура CNN-GRU	99,3%	4%
[27]	Оптимизированная CNN с предобработкой и каскадным классификатором	99,95%	0,65%

Также были определены параметры формирования многоканальных матриц, обеспечивающие лучшее качество работы модели сверточной нейронной сети. Установлено, что увеличение размера матрицы (количества анализируемых клавиш) сверх 25-30 не дает существенного прироста качества. Наилучшие результаты в большинстве архитектур были достигнуты при использовании только среднего выборочного значения, в то время как расширенный набор статистических характеристик (среднеквадратичное отклонение,

асимметрия, эксцесс) часто приводил к чрезмерному разреживанию данных и снижению точности.

Кроме того, в результате экспериментального исследования был сделан ряд других выводов.

- Эффективность классических CNN. Классическая сверточная нейронная сеть показала высокую эффективность, достигнув точности 99.2%. Это подтвердило способность CNN успешно обрабатывать разреженные данные, извлекать информативные признаки и игнорировать малоинформативные, несмотря на высокую разреженность матриц.

- Ограничение глубины сетей. Для всех протестированных архитектур было выявлено, что использование излишне глубоких сетей (глубиной более 2 блоков) является контрпродуктивным и приводит к значительному снижению качества распознавания.

- Сравнение с аналогами. Проведенное сравнение с существующими аналогами показало, что разработанные модели, в особенности классическая CNN и разделенная CNN, демонстрируют конкурентоспособные и превосходящие результаты как по метрике точности, так и по EER. Разделенная CNN уступает лишь одному известному аналогу по точности, но превосходит его по EER.

Перспективы дальнейших исследований видятся в более тонкой настройке архитектуры разделенной сверточной сети, исследовании методов компенсации разреженности при использовании полного набора статистических характеристик.

Литература

1. Risto H.N., Graven O.H. Fixed-text keystroke dynamics authentication data set – collection and analysis // *Annals of Telecommunications*. 2024. vol. 79. pp. 731–743. DOI: 10.1007/s12243-024-01039-z.
2. Shadman R., Wahab A.A., Manno M., Lukaszewski M., Hou D., Hussain F. Keystroke Dynamics: Concepts, Techniques, and Applications // *ACM Computing Surveys*. 2025. vol. 57. no. 11. pp. 1–35. DOI: 10.1145/3733103.
3. Shelupanov A., Evsyutin O., Konev A., Kostyuchenko E., Kruchinin D., Nikiforov D. Information Security Methods – Modern Research Directions // *Symmetry*. 2019. vol. 11. no. 2. 150 p. DOI: 10.3390/sym11020150.
4. Давыденко С.А., Костюченко Е.Ю., Новиков С.Н. Оценивание информативности признаков в наборах данных для проведения продлённой аутентификации // *Информатика и автоматизация*. 2024. Т. 23. №1. С. 65–100. DOI: 10.15622/ia.23.1.3.
5. Zateev S., Shelupanov A. Keyboard Handwriting as a Factor of User Authentication // *Lecture Notes in Networks and Systems*. Springer. 2024. vol. 942. pp. 155–167. DOI: 10.1007/978-3-031-55349-3_13.
6. Затеев С.В. Продленная аутентификация на основе анализа клавиатурного почерка // *Теория и практика обеспечения информационной безопасности: Сб. научн. тр. XX Международной конференции студентов, аспирантов и молодых ученых*. 2023. Т. 7. С. 116–123.

7. Monaco J.V., Bakelman N., Cha S.-H. Tappert C.C. Developing a keystroke biometric system for continual authentication of computer users // *Proceedings of European Intelligence and Security Informatics Conference (EISIC)*. 2012. pp. 210–216. DOI: 10.1109/EISIC.2012.58.
8. Altwajry N. Authentication by Keystroke Dynamics: The Influence of Typing Language // *Applied Sciences*. 2023. vol. 13. no. 20. 11478 p. DOI: 10.3390/app132011478.
9. Bailey K.O., Okolika J.S., Peterson G.L. User identification and authentication using multi-modal behavioral biometrics // *Computers & Security*. 2014. vol. 43. pp. 77–89. DOI: 10.1016/j.cose.2014.03.005.
10. Sharma A., Jurecek M., Stamp M. Keystroke Dynamics for User Identification // *Machine Learning, Deep Learning and AI for Cybersecurity*. Springer. 2025. pp. 601–622. DOI: 10.1007/978-3-031-83157-7_21.
11. Wycislik L., Wylezek P., Momot A. The Improved Biometric Identification of Keystroke Dynamics Based on Deep Learning Approaches // *Sensors*. 2024. vol. 24. no. 12. 3763 p. DOI: 10.3390/s24123763.
12. Spata M.O., Russo V.M., Ortis A., Battiato S. A New Pipeline for Snooping Keystroke Based on Deep Learning Algorithm // *IEEE Access*. 2025. vol. 13. pp. 24498–24514. DOI: 10.1109/ACCESS.2025.3536877.
13. Kaur D., De Carvalho G.H.S., Dividino R., Woungang I., Anpalagan A. Novel Explainable CNN-LightGBM Model for Smartphone Continuous Authentication // *IEEE Access*. 2026. vol. 14. pp. 45826–45843. DOI: 10.1109/ACCESS.2026.3672372.
14. Chang H.-C., Li J., Wu C.-S., Stamp M. Machine Learning and Deep Learning for Fixed-Text Keystroke Dynamics // *Advances in Information Security*. Springer. 2022. vol. 54. pp. 309–329. DOI: 10.1007/978-3-030-97087-1_13.
15. Muralidharan A., Eaman A., Hassan E. A Comparative Analysis of Machine Learning Models for Behavioral Biometric Authentication using Keystroke Dynamics // *Proceedings of the 20th International Conference on Future Networks and Communications*. Procedia Computer Science. 2025. vol. 265. pp. 116–123. DOI: 10.1016/j.procs.2025.07.163.
16. Krishnamoorthy S., Rueda L., Saad S., Elmiligi H. Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning // *Proceedings of 2nd International Conference on Biometric Engineering and Applications (ICBEA '18)*. 2018. pp. 50–57. DOI: 10.1145/3230820.3230829.
17. Bleha S.A., Knopp J., Obaidat M.S. Performance of the Perceptron algorithm for the classification of computer users // *Proceedings of ACM/SIGAPP Symposium on Applied Computing: Technological Challenges of the 1990s*. 1992. pp. 863–866.
18. Stylios I., Skalkos A., Kokolakis S., Karyda M. BioPrivacy: Development of a Keystroke Dynamics Continuous Authentication System // *Lecture Notes in Computer Science*. Springer. 2021. vol. 13106. pp. 158–170. DOI: 10.1007/978-3-030-95484-0_10.
19. Wahab A., Hou D., Schuckers S., Barbir, A. Utilizing Keystroke Dynamics as Additional Security Measure to Protect Account Recovery Mechanism // *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP)*. 2021. vol. 1. pp. 33–42. DOI: 10.5220/0010191200330042.
20. Acien A., Morales A., Monaco J.V., Vera-Rodriguez R., Fierrez J. TypeNet: Deep learning keystroke biometrics // *IEEE Transactions on Biometrics, Behavior, and Identity Science*. 2021. vol. 4. no. 1. pp. 57–70. DOI: 10.1109/TBIOM.2021.3112540.
21. Li J., Chang H.-C., Stamp M. Free-Text Keystroke Dynamics for User Authentication // *Advances in Information Security*. Springer. 2022. vol. 54. pp. 357–380. DOI: 10.1007/978-3-030-97087-1_15.
22. Gonzalez N., Stragapede G., Vera-Rodriguez R., Tolosana R. Type2Branch: Keystroke Biometrics Based on a Dual-Branch Architecture With Attention

- Mechanisms and Set2set Loss // IEEE Transactions on Information Forensics and Security. 2025. vol. 20. pp. 5859–5871. DOI: 10.1109/TIFS.2025.3574992.
23. Stragapede G., Delgado-Santos P., Tolosana R., Vera-Rodriguez R., Guest R., Morales A. TypeFormer: Transformers for mobile keystroke biometrics // Neural Computing and Applications. 2024. vol. 36. pp. 18531–18545. DOI: 10.1007/s00521-024-10140-2.
24. Neacsu T., Poncu T., Ruseti S., Dascalu M. DoubleStrokeNet: Bigram-level keystroke authentication // Electronics. 2023. vol. 12. no. 20. 4309 p. DOI: 10.3390/electronics12204309.
25. Kasprowski P., Borowska Z., Harezlak K. Biometric Identification Based on Keystroke Dynamics // Sensors. 2022. vol. 22. no. 9. 3158 p. DOI: 10.3390/s22093158.
26. Chang H.-C., Li J., Stamp M. Machine Learning-Based Analysis of Free-Text Keystroke Dynamics // Advances in Information Security. Springer. 2022. vol. 54. pp. 331–356. DOI: 10.1007/978-3-030-97087-1_14.
27. AbdelRaouf H., Chelloug S.A., Muthanna A., Semaary N., Amin K., Ibrahim M. Efficient Convolutional Neural Network-Based Keystroke Dynamics for Boosting User Authentication // Sensors. 2023. vol. 23. no. 10. 4898 p. DOI: 10.3390/s23104898.

Затеев Станислав Вадимович — младший научный сотрудник, научно-инжиниринговый центр «интеллектуальные системы доверенного взаимодействия», Федеральное государственное автономное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ФГАОУ ВО «ТУСУР»). Область научных интересов: искусственный интеллект и машинное обучение, анализ данных. Число научных публикаций — 4. zateev.stanislav@gmail.com; пр. Ленина, 40, 634050, Томск, Россия; р.т.: +7(931)491-7404.

Костюченко Евгений Юрьевич — канд. техн. наук, заведующий лабораторией, лаборатория съёма, анализа и управления биологическими сигналами; доцент, кафедра комплексной информационной безопасности электронно-вычислительных систем, Федеральное государственное автономное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ФГАОУ ВО «ТУСУР»). Область научных интересов: искусственный интеллект и машинное обучение, обработка речи, биометрия, анализ данных. Число научных публикаций — 154. key@fb.tusur.ru; пр. Ленина, 40, 634050, Томск, Россия; р.т.: +7(382)270-1529.

Шелупанов Александр Александрович — д-р техн. наук, профессор, член-корреспондент РАН, директор, институт системной интеграции и безопасности; заведующий кафедрой, кафедра комплексной информационной безопасности электронно-вычислительных систем, Федеральное государственное автономное образовательное учреждение высшего образования «Томский государственный университет систем управления и радиоэлектроники» (ФГАОУ ВО «ТУСУР»). Область научных интересов: информационная безопасность, математическое моделирование. Число научных публикаций — 437. saa@tusur.ru; пр. Ленина, 40, 634050, Томск, Россия; р.т.: +7(382)290-7155.

Поддержка исследований. Работа выполнена при поддержке Министерства науки и высшего образования РФ: FEWM-2026-0009 (ТУСУР).

S. ZATEEV, E. KOSTYUCHENKO, A. SHELUPANOV
**COMPARATIVE ANALYSIS OF APPROACHES TO
CONVOLUTIONAL NEURAL NETWORK ARCHITECTURE
DESIGN FOR KEYSTROKE DYNAMICS ANALYSIS**

Zateev S., Kostyuchenko E., Shelupanov A. Comparative Analysis of Approaches to Convolutional Neural Network Architecture Design for Keystroke Dynamics Analysis.

Abstract. In the context of widespread digitalization and the increasing frequency of confidential information compromise incidents, the relevance of developing reliable authentication systems serving as the primary line of defense becomes critically important. Behavioral biometric systems present a promising solution to the problems associated with loss, theft, or unauthorized use of static identifiers. In particular, methods based on keystroke dynamics analysis enable continuous and transparent user authentication throughout an entire work session by analyzing unique and difficult-to-forge behavioral patterns. This research direction is characterized by a combination of a high level of security with relatively moderate implementation costs and high user convenience. The aim of this study is to conduct a comparative analysis of various approaches to the design and construction of convolutional neural network architectures optimized for processing sparse data describing keystroke dynamics. The experimental work revealed that convolutional neural networks demonstrate exceptionally high verification accuracy, reaching 99%, despite the fact that the input data generated during preprocessing exhibit significant sparsity. The best results within the framework of this study were achieved using an architecture based on a depthwise separable convolution mechanism, which proved to be effective for handling this specific data type.

Keywords: authentication, behavioral biometrics, keystroke dynamics, sparse data, convolutional neural networks.

References

1. Risto H.N., Graven O.H. Fixed-text keystroke dynamics authentication data set – collection and analysis. *Annals of Telecommunications*. 2024. vol. 79. pp. 731–743. DOI: 10.1007/s12243-024-01039-z.
2. Shadman R., Wahab A.A., Manno M., Lukaszewski M., Hou D., Hussain F. Keystroke Dynamics: Concepts, Techniques, and Applications. *ACM Computing Surveys*. 2025. vol. 57. no. 11. pp. 1–35. DOI: 10.1145/3733103.
3. Shelupanov A., Evsyutin O., Konev A., Kostyuchenko E., Kruchinin D., Nikiforov D. Information Security Methods – Modern Research Directions. *Symmetry*. 2019. vol. 11. no. 2. 150 p. DOI: 10.3390/sym11020150.
4. Davydenko S., Kostyuchenko E., Novikov S. [Evaluation of the Informativeness of Features in Datasets for Continuous Verification]. *Informatika i avtomatizatsiya – Informatics and Automation*. 2024. vol. 23. no. 1. pp. 65–100. DOI: 10.15622/ia.23.1.3. (In Russ.).
5. Zateev S., Shelupanov A. Keyboard Handwriting as a Factor of User Authentication. *Lecture Notes in Networks and Systems*. Springer. 2024. vol. 942. pp. 155–167. DOI: 10.1007/978-3-031-55349-3_13.
6. Zateev S. [Extended User Authentication Based on Keyboard Handwriting Analysis]. *Teoriya i praktika obespecheniya informatsionnoy bezopasnosti: Sb. nauchn. tr. XX Mezhdunarodnoy konferentsii studentov, aspirantov i molodykh uchenykh [Theory and practice of information security : Collected papers]*. 2023. vol. 7. pp. 116–123. (In Russ.).

7. Monaco J.V., Bakelman N., Cha S.-H. Tappert C.C. Developing a keystroke biometric system for continual authentication of computer users. *Proceedings of European Intelligence and Security Informatics Conference (EISIC)*. 2012. pp. 210–216. DOI: 10.1109/EISIC.2012.58.
8. Altwaijry N. Authentication by Keystroke Dynamics: The Influence of Typing Language. *Applied Sciences*. 2023. vol. 13. no. 20. 11478 p. DOI: 10.3390/app132011478.
9. Bailey K.O., Okolica J.S., Peterson G.L. User identification and authentication using multi-modal behavioral biometrics. *Computers & Security*. 2014. vol. 43. pp. 77–89. DOI: 10.1016/j.cose.2014.03.005.
10. Sharma A., Jurecek M., Stamp M. Keystroke Dynamics for User Identification. *Machine Learning, Deep Learning and AI for Cybersecurity*. Springer. 2025. pp. 601–622. DOI: 10.1007/978-3-031-83157-7_21.
11. Wycislik L., Wylezek P., Momot A. The Improved Biometric Identification of Keystroke Dynamics Based on Deep Learning Approaches. *Sensors*. 2024. vol. 24. no. 12. 3763 p. DOI: 10.3390/s24123763.
12. Spata M.O., Russo V.M., Ortis A., Battiato S. A New Pipeline for Snooping Keystroke Based on Deep Learning Algorithm. *IEEE Access*. 2025. vol. 13. pp. 24498–24514. DOI: 10.1109/ACCESS.2025.3536877.
13. Kaur D., De Carvalho G.H.S., Dividino R., Woungang I., Anpalagan A. Novel Explainable CNN-LightGBM Model for Smartphone Continuous Authentication. *IEEE Access*. 2026. vol. 14. pp. 45826–45843. DOI: 10.1109/ACCESS.2026.3672372.
14. Chang H.-C., Li J., Wu C.-S., Stamp M. Machine Learning and Deep Learning for Fixed-Text Keystroke Dynamics. *Advances in Information Security*. Springer. 2022. vol. 54. pp. 309–329. DOI: 10.1007/978-3-030-97087-1_13.
15. Muralidharan A., Eaman A., Hassan E. A Comparative Analysis of Machine Learning Models for Behavioral Biometric Authentication using Keystroke Dynamics. *Proceedings of the 20th International Conference on Future Networks and Communications*. *Procedia Computer Science*. 2025. vol. 265. pp. 116–123. DOI: 10.1016/j.procs.2025.07.163.
16. Krishnamoorthy S., Rueda L., Saad S., Elmiligi H. Identification of User Behavioral Biometrics for Authentication Using Keystroke Dynamics and Machine Learning. *Proceedings of 2nd International Conference on Biometric Engineering and Applications (ICBEA '18)*. 2018. pp. 50–57. DOI: 10.1145/3230820.3230829.
17. Bleha S.A., Knopp J., Obaidat M.S. Performance of the Perceptron algorithm for the classification of computer users. *Proceedings of ACM/SIGAPP Symposium on Applied Computing: Technological Challenges of the 1990s*. 1992. pp. 863–866.
18. Stylios I., Skalkos A., Kokolakis S., Karyda M. BioPrivacy: Development of a Keystroke Dynamics Continuous Authentication System. *Lecture Notes in Computer Science*. Springer. 2021. vol. 13106. pp. 158–170. DOI: 10.1007/978-3-030-95484-0_10.
19. Wahab A., Hou D., Schuckers S., Barbir, A. Utilizing Keystroke Dynamics as Additional Security Measure to Protect Account Recovery Mechanism. *Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP)*. 2021. vol. 1. pp. 33–42. DOI: 10.5220/0010191200330042.
20. Acien A., Morales A., Monaco J.V., Vera-Rodriguez R., Fierrez J. TypeNet: Deep learning keystroke biometrics. *IEEE Transactions on Biometrics, Behavior, and Identity Science*. 2021. vol. 4. no. 1. pp. 57–70. DOI: 10.1109/TBIOM.2021.3112540.
21. Li J., Chang H.-C., Stamp M. Free-Text Keystroke Dynamics for User Authentication. *Advances in Information Security*. Springer. 2022. vol. 54. pp. 357–380. DOI: 10.1007/978-3-030-97087-1_15.
22. Gonzalez N., Stragapede G., Vera-Rodriguez R., Tolosana R. Type2Branch: Keystroke Biometrics Based on a Dual-Branch Architecture With Attention

- Mechanisms and Set2set Loss. IEEE Transactions on Information Forensics and Security. 2025. vol. 20. pp. 5859–5871. DOI: 10.1109/TIFS.2025.3574992.
23. Stragapede G., Delgado-Santos P., Tolosana R., Vera-Rodriguez R., Guest R., Morales A. TypeFormer: Transformers for mobile keystroke biometrics. Neural Computing and Applications. 2024. vol. 36. pp. 18531–18545. DOI: 10.1007/s00521-024-10140-2.
 24. Neacsu T., Poncu T., Ruseti S., Dascalu M. DoubleStrokeNet: Bigram-level keystroke authentication. Electronics. 2023. vol. 12. no. 20. 4309 p. DOI: 10.3390/electronics12204309.
 25. Kasprowski P., Borowska Z., Harezlak K. Biometric Identification Based on Keystroke Dynamics. Sensors. 2022. vol. 22. no. 9. 3158 p. DOI: 10.3390/s22093158.
 26. Chang H.-C., Li J., Stamp M. Machine Learning-Based Analysis of Free-Text Keystroke Dynamics. Advances in Information Security. Springer. 2022. vol. 54. pp. 331–356. DOI: 10.1007/978-3-030-97087-1_14.
 27. AbdelRaouf H., Chelloug S.A., Muthanna A., Semary N., Amin K., Ibrahim M. Efficient Convolutional Neural Network-Based Keystroke Dynamics for Boosting User Authentication. Sensors. 2023. vol. 23. no. 10. 4898 p. DOI: 10.3390/s23104898.

Zateev Stanislav — Junior Research Associate, Scientific and Engineering Center "Intelligent Trusted Interaction Systems", Federal State Autonomous Educational Institution of Higher Education "Tomsk State University of Control Systems and Radioelectronics" (TUSUR). Research interests: artificial intelligence and machine learning, data analysis. The number of publications — 4. zateev.stanislav@gmail.com; 40, Lenin Ave., 634050, Tomsk, Russia; office phone: +7(931)491-7404.

Kostyuchenko Evgeniy — Ph.D., Head of the Laboratory, Laboratory for the Removal, Analysis and Control of Biological Signals; Associate Professor, Department of Integrated Information Security of Electronic Computing Systems, Federal State Autonomous Educational Institution of Higher Education "Tomsk State University of Control Systems and Radioelectronics" (TUSUR). Research interests: artificial intelligence and machine learning, speech processing, biometrics, data analysis. The number of publications — 154. key@fb.tusur.ru; 40, Lenin Ave., 634050, Tomsk, Russia; office phone: +7(382)270-1529.

Shelupanov Alexander — Ph.D., Dr.Sci., Professor, Corresponding Member of RAS, Director, Institute of System Integration and Security; Head of the Department, Department of Integrated Information Security of Electronic Computing Systems, Federal State Autonomous Educational Institution of Higher Education "Tomsk State University of Control Systems and Radioelectronics" (TUSUR). Research interests: information security, mathematical modeling. The number of publications — 437. saa@tusur.ru; 40, Lenin Ave., 634050, Tomsk, Russia; office phone: +7(382)290-7155.

Acknowledgements. The work was supported by the Ministry of Science and Higher Education of the Russian Federation: FEWM-2026-0009 (TUSUR).