УДК 004.89 **DOI** 10.15622/ia.25.3.10

Н.Л.Харина, М.Л.Долженкова, З.Б.Иминова

ЗАЩИЩЕННАЯ СИСТЕМА БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ ДЛЯ ВСТРАИВАЕМЫХ СИСТЕМ С ОГРАНИЧЕННЫМИ ВЫЧИСЛИТЕЛЬНЫМИ РЕСУРСАМИ

Харина Н.Л., Долженкова М.Л., Иминова З.Б. **Защищенная система биометрической аутентификации для встраиваемых систем с ограниченными вычислительными ресурсами.**

Аннотация. В настоящее время технологии биометрической аутентификации такие как распознавание лица, отпечатков пальцев, радужной оболочки глаза и вен ладони, активно применяются в банковских приложениях, медицинских системах, комплексах контроля доступа и государственных информационных ресурсах. Использование таких технологий должно сопровождаться защитой биометрической информации при обработке и хранении особенно в условиях растущего количества целевых атак на персональные данные. Одним из перспективных подходов к обеспечению безопасности биометрической информации является использование гомоморфного шифрования. В работе рассматривается система автономной защищенной биометрической аутентификации по рисунку вен ладони пользователя в ближнем инфракрасном спектре для встроенных систем, реализуемых с использованием технологии обеспечения конфиденциальности для защиты биометрических данных. Проведенные исследования показали практическую реализуемость системы биометрической аутентификации с применением легковесной сиамской нейронной сети для выделения вектора признаков и гомоморфного шифрования, обеспечивающего конфиденциальность во встраиваемых системах на процессорах с ограниченными вычислительными ресурсами на основе одноплатных компьютеров, таких как Raspberry Pi. Подтверждена устойчивость к искажениям, включая повороты, шум, смещения и варьирование параметров шифрования. Показатели эффективности разработанной системы оценивались на сборном датасете, состоящем из изображений датасетов CASIA-MS-PalmprintV1 и Tongji Contactless Palmvein Dataset и составляют: точность классификации – 98,2%, EER – 0,73 %, AUC – 0,96, время – 1,2 секунды, что соответствует уровню требований к подобным системам. Анализ результатов показывает, что разработанная система уступает по точности клиент-серверным решениям, построенным на тяжеловесных сверточных нейронных сетях из-за ограниченности в вычислительных ресурсах и как следствие необходимости применения легковесной нейронной сети, но при этом обеспечена защищенная обработка биометрических данных с сохранением допустимого времени отклика. Сокращение времени обработки при реализации на одноплатных компьютерах может быть реализовано как использованием специализированных вычислительных ускорителей, так и применением других библиотек, поддерживающих гомоморфные вычисления, менее требовательных к вычислительным ресурсам.

Ключевые слова: биометрическая аутентификация, обработка изображений, сверточная нейронная сеть, сиамская нейронная сеть, конфиденциальная обработка биометрических признаков, гомоморфное шифрование.

1. Введение. Современные технологии биометрической аутентификации становятся важнейшим компонентом информационной безопасности, обеспечивая надежный и удобный способ подтверждения личности пользователя при доступе к цифровым системам.

Биометрические методы, такие как распознавание лица, отпечатков пальцев, радужной оболочки глаза и вен ладони, активно применяются в банковских приложениях, медицинских системах, комплексах контроля доступа и государственных информационных ресурсах [1 – 3].

В последнее время широкое распространение получил метод аутентификации по рисунку вен ладони. Данный вид биометрии является неизменным в течение жизни пользователя, не требует дорогостоящего оборудования для реализации, демонстрирует высокую точность, устойчивость к подделке и низкий уровень ложных срабатываний. Обзор разработок с использованием данного вида биометрии и технологий искусственного интеллекта для выделения признаков и сравнения с базовыми шаблонами демонстрирует актуальность данной технологии, высокие показатели точности распознавания и идентификации пользователя. Среди таких разработок можно выделить некоторые работы. Авторы [4] предлагают модель аутентификации по венам ладони с использованием сверточных нейронных сетей (CNN) с применением байесовской оптимизации. В работе [5] авторы используют адаптивный фильтр Габора и триплет CNN. Авторы [6] предлагают подход MSMDGAN® CNN, который состоит из многомасштабной и многонаправленной генеративно-состязательной сети (MSMDGAN) для аугментации данных и CNN для идентификации вен на ладони. В работе [7] приведен пример применения CNN на основе ZFNet архитектуры для распознавания рисунка вен ладони. Авторы [8] разработали Focal Contrastive Palm Vein Network для построения биометрической системы аутентификации. В работе [9] предложен многомасштабный преобразователь вен (MSVT) для обучения устойчивым и многомасштабным признакам, который состоит из сверточного блока, захватывающего локальную информацию, и блока самовнимания, извлекающего масштабные зависимости между изображениями с разными масштабами, для учета взаимосвязи между метками использована графовая сверточная сеть (GCNLE). Авторы [10] предлагают подход VeinGuard, состоящий из локальной трансформерной генеративно-состязательной сети (LTGAN), которая обучается распределению изображений вен и генерирует высококачественные изображения вен ладони, и очистителя, состоящего из обучаемой остаточной сети и предварительно обученного генератора на основе LTGAN для удаления частей изображений, не относящихся к рисунку вен. Авторы [11] провели сравнительный анализ существующих моделей CNN, таких как LeNet, AlexNet, ResNet, ZFNet, выделяя по производительности ZFNet.

Большинство из рассмотренных вариантов используют тяжеловесные модели, что оправдано для повышения точности распознавания, такие алгоритмы используются для построения распределенных и клиент-серверных архитектур систем биометрической аутентификации (СБА). Однако наряду с распределенными и клиент-серверными архитектурами СБА находят свое применение автономные или встроенные системы [12], требующие применения легковесных нейронных сетей из-за ограниченных вычислительных ресурсов, но таких разработок не так много.

Наряду с очевидными преимуществами, СБА предъявляют особые требования к защите пользовательских данных. Биометрические признаки являются уникальными и неизменяемыми, поэтому утечка может привести к необратимым последствиям. Это делает конфиденциальную обработку и хранение биометрических данных критически важным аспектом архитектуры подобных систем, особенно в условиях растущего количества целевых атак на персональные данные [13 – 15]. Традиционные алгоритмы шифрования не применимы к биометрическим данным, так как компрометация секретного ключа приводит к утечке биометрических данных. Более того, небольшие изменения в исходных биометрических данных, такие как неизбежные расхождения между несколькими измерениями биометрических данных, относящихся к одной и той же характеристике одного и того же человека, приводят к кардинальным изменениям в зашифрованных данных. Поэтому биометрические данные невозможно обрабатывать и сравнивать в зашифрованном виде и необходимо их расшифровать перед сравнением, что создает риск их использования потенциальными злоумышленниками. Следовательно, для защиты биометрических данных требуются другие технологии повышения конфиденциальности биометрического распознавания. К ним относятся такие технологии как:

– отменяемые биометрические данные – преднамеренное повторяющееся искажение исходных биометрических данных, которые позволяют сравнивать биометрические данные в преобразованном виде;

– биометрические криптосистемы – предназначены для безопасной привязки цифрового ключа к биометрическим данным или генерации цифрового ключа из биометрических данных;

– гомоморфное шифрование – технология, позволяющая выполнять операции над зашифрованными данными без промежуточного расшифровывания [16];

– применение нечетких экстракторов для формирования ключа для стандартных криптографических методов [17, 18].

Применение нечетких экстракторов заключается в использовании кодов, способных обнаруживать и корректировать ошибки.

При выборе технологии должны соблюдаться основные требования к конфиденциальности биометрических данных:

– необратимость: восстановление исходного биометрического шаблона из сохраненных справочных данных, т.е. защищенного шаблона, должно быть трудным в вычислительном отношении, в то время как создание защищенного биометрического шаблона должно быть простым;

– несвязность: разные версии защищенных биометрических шаблонов могут быть созданы на основе одних и тех же биометрических данных (возможность обновления), в то время как защищенные шаблоны не должны допускать перекрестного сопоставления (разнообразия) [19].

Одним из наиболее перспективных подходов к обеспечению безопасности биометрической информации является использование гомоморфного шифрования – криптографической технологии, позволяющей выполнять операции над зашифрованными данными без предварительной расшифровки. Такой подход предоставляет возможность защищенной обработки данных на всех этапах жизненного цикла: от хранения и передачи до сравнения признаков. На фоне активного внедрения методов машинного обучения интеграция гомоморфного шифрования в биометрические системы аутентификации получила широкое распространение в научных и прикладных разработках, например, в [20] представлена СБА по радужке глаз с применением гомоморфного шифрования, в [21, 22] рассмотрены варианты защищенной биометрической аутентификации по лицу. В работе [23] авторы предложили использовать защищенную гомоморфным шифрованием аутентификацию по лицу для IoT систем, в [24] авторы оценивают устойчивость к атакам СБА на основе отпечатка пальца, рассматривают варианты защиты биометрических данных. В [25] авторы провели обзор моделей глубокого обучения, применяемых для аутентификации пользователей по рисунку вен пальца и ладони за последние 5 лет, демонстрирующий высокую точность аутентификации пользователей при надежной защите биометрических данных.

2. Постановка задачи. Требуется разработать автономную СБА для встроенных систем, обеспечивающую конфиденциальность биометрических данных. В качестве биометрического признака использовать рисунок вен ладони пользователя.

2.1. Математическая постановка задачи.

Входные данные. На вход системы поступает изображение ладони пользователя, полученное с камеры ближнего инфракрасного диапазона (NIR):

$$I_{raw}(x, y) \in R_{H \times W},$$

где: H, W – высота и ширина исходного изображения, $I_{raw}(x,y)$ – интенсивность пикселя в оттенках серого.

Выходные данные. На выходе система принимает бинарное решение:

$$d \in \{0,1\},$$

где: $d = 1$ – аутентификация успешна (пользователь подтверждён), $d = 0$ – аутентификация не успешна (доступ запрещён).

Этапы обработки данных. Выделение области интереса (ROI) – прямоугольная область ладони, содержащая венозный рисунок:

$$ROI = CropAndRotate(I_{raw}, \theta, P_1, P_2),$$

где: P_1, $P2$ – опорные точки (впадины между пальцами), Θ – угол поворота для нормализации.

Бинаризация ROI с помощью пороговой обработки:

$$ROI\_BINARY(x, y) = \begin{cases} 1, & \textit{если } ROI(x, y) \geq T, \\ 0, & \textit{если } ROI(x, y) < T. \end{cases}$$

Скелетизация бинарного изображения *ROI_BINARY*:

$$ROI\_Skel = Skeletonize(ROI\_BINARY),$$

где *ROI_Skel* – бинарное изображение венозного рисунка толщиной в один пиксель.

Извлечение признаков с помощью сиамской нейросети. Скелетизированное изображение *ROI*_Skel подаётся на вход свёрточной нейросети *f*:

$$v = f(ROI\_Skel) \in R_{128},$$

где v – вектор признаков длиной 128, компактно описывающий венозный рисунок.

Квантование и гомоморфное шифрование. Вектор признаков v нормализуется к диапазону $[-1,1]$ и квантуется в целые числа с фиксированной разрядностью n:

$$v_q = Quantize(v) \in Z^n.$$

Затем каждый элемент шифруется с использованием открытого ключа *public_key* в рамках схемы полного гомоморфного шифрования (FHE), поддерживающей сложение и умножение:

$$c = Enc_{public\_key}(v_q) \in C^n,$$

где C – пространство шифротекстов.

Сравнение с эталоном в зашифрованном виде. Для аутентификации выполняется конкатенация зашифрованного входного вектора c и эталонного зашифрованного вектора c_{ref}, соответствующего идентификатору пользователя id:

$$c_{concat} = c \| c_{ref},$$

где || – операция конкатенации, выполняемая над шифротекстами.

Полученный вектор подаётся на классификатор g, реализованный как часть свёрточной нейросети, адаптированной для работы с зашифрованными данными:

$$w = g(c_{concat}) \in [0,1],$$

где w – вероятность принадлежности одной и той же ладони.

Принятие решения. Итоговое решение принимается путём сравнения с порогом τ:

$$d = \begin{cases} 1, & \text{если } w \geq \tau, \\ 0, & \text{если } w < \tau. \end{cases}$$

Порог τ подбирается эмпирически на этапе валидации как значение, обеспечивающее баланс между вероятностями ложного допуска и ложного отказа.

2.2. Аппаратно-программная платформа:

Камера ближнего инфракрасного диапазона (NIR) для захвата изображений вен ладони.

СБА должна функционировать на устройстве с ограниченными вычислительными ресурсами – одноплатный компьютер (Raspberry Pi 4/5 или аналог).

Операционная система: Linux (Raspberry Pi OS).

2.3. Функциональные требования:

1. Захват и предобработка изображения ладони пользователя в NIR-спектре.
2. Извлечение биометрического шаблона.
3. Извлечение вектора признаков.
4. Выполнение криптографического преобразования над вектором признаков для обеспечения защищенной обработки и хранения эталонных шаблонов в базе данных.
5. Сравнение входного биометрического шаблона с эталонным шаблоном, хранящимся в системе.
6. Принятие бинарного решения на основе порога схожести (Аутентификация успешна/неуспешна).

2.4. Требования к производительности и точности:

1. Время выполнения полного цикла аутентификации ≤ 2 секунды для реализации на ПК и ≤ 4 секунды при реализации на Raspberry Pi 4/5 или аналог.
2. Точность классификации (аутентификации) – Accuracy $\geq 98\%$ (на тестовой выборке).
3. Вероятность ошибок первого рода (FRR) и второго рода (FAR) должны быть минимизированы при соблюдении условия точности.

2.5. Требования к безопасности и конфиденциальности:

1. Биометрические шаблоны (исходные и эталонные) должны храниться и обрабатываться только в защищенном (необратимом) виде.
2. Метод криптографического преобразования – полное гомоморфное шифрование.
3. Криптографические ключи не должны покидать устройство.

3. Структура системы биометрической аутентификации.

Общая структура системы биометрической аутентификации представлена на рисунке 1 и состоит из следующих модулей:

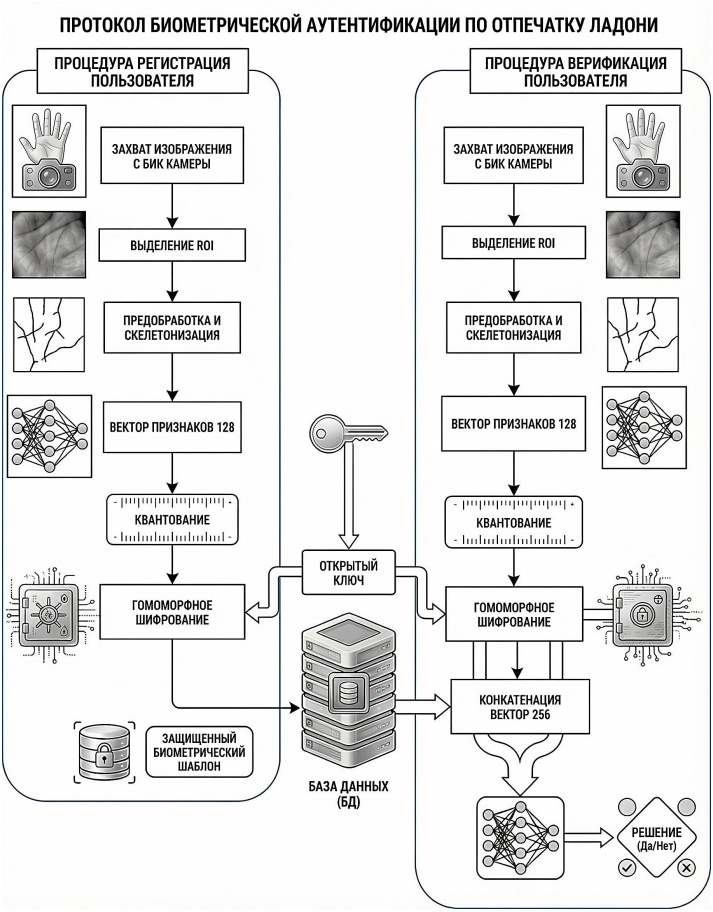

Рис. 1. Структура системы биометрической аутентификации

– модуль захвата и предобработки изображений ладони в инфракрасном спектре;

– модуль выделения области интереса (ROI) и предварительной обработки изображения (адаптивное выравнивание гистограммы с ограниченным контрастом, бинаризация, скелетизация);

– модуль извлечения признаков с использованием сверточной нейросети;

– модуль квантования и гомоморфного шифрования признаков с использованием открытого ключа;

– модуль сравнения с эталоном и принятия решения сверточной моделью.

СБА может работать в двух режимах: внесение биометрического шаблона пользователя в базу данных и режим верификации пользователя.

В режиме внесения данных изображение с БИК камеры поступает в блок выделения области интереса (ROI), проходит все этапы предобработки, результатом является скелет вен ладони. Далее с использованием сверточной нейросети осуществляется выделение вектора признаков с последующим квантованием и зашифрованием. Защищенный биометрический шаблон подлежит записи в базу данных.

В режиме аутентификации пользователь предъявляет свой идентификатор и прикладывает ладонь к сканеру. Изображение ладони проходит описанные выше процедуры и для вынесения решения об аутентификации происходит объединение защищенного биометрического шаблона пользователя с его эталонным из базы данных.

4. Модуль выделения области интереса и предварительной обработки изображения. Выделение области интереса является базовым этапом в структуре биометрической СБА. Цель данного этапа – локализация центральной части ладони, содержащей устойчивую и информативную васкулярную структуру, а также нормализация положения руки по масштабу и ориентации. В рамках проектируемой архитектуры применяется геометрический алгоритм, включающий бинаризацию, морфологическую обработку, определение опорных точек и коррекцию наклона изображения [26].

На вход подается полутоновое изображение ладони с NIR камеры (Рис. 2(a)). Для выделения объекта интереса применяется метод автоматической бинаризации по критерию Otsu. Алгоритм Otsu определяет пороговое значение яркости, при котором достигается максимальное разделение между классами «объект» (ладонь) и «фон» (Рис. 2(b)). Применение данной методики позволяет адаптировать процесс сегментации к различным условиям освещенности и яркости.

К полученному бинарному изображению применяется морфологическая эрозия с ядром [0,1,0;1,1,1;0,1,0], за которой следует операция поэлементного вычитания из исходной бинарной маски. Результатом является тонкий замкнутый контур ладони. Далее выполняется фильтрация контуров по длине: строятся контуры всех объектов и удаляются все объекты, кроме объекта с максимальной длиной. Это позволяет устранить шум и оставить только основной контур руки (Рис. 2(c)).

После получения контура ладони рассчитывается координата центра запястья, определяемая как середина между двумя крайними точками нижней границы контура. Далее вычисляются так называемые особые точки ладони – впадины между пальцами, в частности между указательным и средним, а также между безымянным и мизинцем. Для поиска проводится полный обход внешнего контура, в ходе которого для каждой точки измеряется расстояние до центра запястья. По сформированному профилю расстояний осуществляется сглаживание и выявление локальных минимумов, соответствующих впадинам между пальцами. Эти точки служат ориентирами для выравнивания изображения.

На основе координат найденных особых точек определяется угол наклона ладони относительно горизонтальной оси (Рис. 2(d)). Изображение поворачивается таким образом, чтобы линия, соединяющая особые точки, стала горизонтальной. Это позволяет устранить наклон руки при захвате и привести все изображения к единой ориентации (Рис. 2(f)).

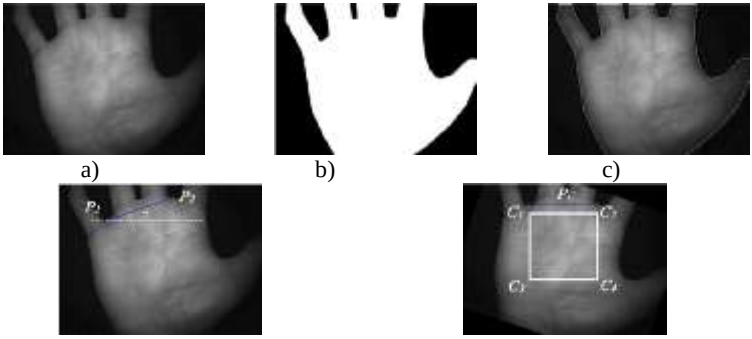

Рис. 2. Процесс выделения ROI: a – исходное изображение; b – бинаризация; c – определение контура; d – определение угла наклона; f – выделение прямоугольной области

После коррекции положения определяется прямоугольная область интереса. Ее верхняя граница проходит через линию, соединяющую найденные впадины между пальцами. Левые и правые границы определяются как вертикальные линии, проходящие через соответствующие особые точки. Нижняя граница устанавливается на фиксированном расстоянии вниз от линии впадин, определенном эмпирически на основе анализа анатомических особенностей.

В результате формируется прямоугольная ROI, содержащая центральную часть ладони и исключающая пальцы и запястье (Рис. 3(a)).

Для усиления видимости сосудистых структур внутри ROI осуществляется фильтрация последовательным применением следующих методов: контрастная ограниченная адаптивная коррекция гистограммы (CLAHE) с параметрами clipLimit=2.0, tileGridSize=(8,8), позволяющая увеличить контраст изображения без значительного усиления шума; медианное размытие (Median Blur) с ядром размытия (3,3), что позволяет уменьшить уровень шумов; размытие по Гауссу (Gaussian Blur), с ядром размытия (3,3), что позволяет уменьшить уровень шумов и снизить детализацию; повторное применение CLAHE с параметрами clipLimit=2.0, tileGridSize=(8,8), для того чтобы увеличить контраст еще сильнее.

Полученное изображение ROI (Рис. 3(a)) дополнительно преобразуется в бинарное представление с целью отделения венозного рисунка от фона. После бинаризации применяется операция скелетизации с помощью алгоритма Zhang-Suen [27], приводящая сосудистые линии к однопиксельной толщине (Рис. 3(b)). Это позволяет сохранить топологическую структуру рисунка и устранить избыточную информацию, не несущую полезных признаков.

a) b)

Рис. 3. Процесс скелетизации: a – ROI; b – результат скелетизации

Скелетизированное бинарное изображение используется в качестве входа для сверточной нейросети на следующем этапе обработки.

5. Модуль извлечения признаков с использованием сверточной нейросети. Извлечение признаков из изображения ладони осуществляется с использованием сверточной нейросети, построенной по архитектуре сиамской модели [28]. Сиамская нейросеть состоит из двух каналов с идентичными весами нейросетей в каждом и применяется обычно для задач измерения сходства между парами входных данных, кроме того, эта модель менее требовательна к вычислительным ресурсам по сравнению с моделями сверточных нейронных сетей, используемых в задачах классификации при построении СБА [4 – 11].

Основная задача нейросетевого блока – преобразование скелетизированного изображения области интереса (ROI) в компактное векторное представление, сохраняющее индивидуальные особенности венозного рисунка. Полученный вектор признаков используется в дальнейших модулях системы для сравнения с эталонными шаблонами в зашифрованной форме.

Модель реализована в виде базовой сверточной нейросети, которая применяется в обеих ветвях сиамской архитектуры с разделяемыми весами, структура представлена на рисунке 4. Структура каждой ветви включает:

1. Четыре сверточных блока:

– слой с 32 фильтрами 3×3, «ReLU», «BatchNormalization», «MaxPooling»;

– слой с 64 фильтрами 3×3, «ReLU», «BatchNormalization», «MaxPooling»;

– слой с 128 фильтрами 3×3, «ReLU», «BatchNormalization», «MaxPooling»;

– слой с 256 фильтрами 3×3, «ReLU», «BatchNormalization»;

2. Глобальный усредняющий пуллинг («Global Average Pooling»);
3. Полносвязный слой из 256 нейронов с «ReLU» и регуляризацией;
4. «Dropout» (p=0.5) для предотвращения переобучения;
5. Полносвязный слой на 128 нейронов с «ReLU».

Выходом каждой ветви является вектор признаков длины 128, компактно описывающий сосудистый рисунок ладони. Два вектора признаков объединяются путем конкатенации в единый вектор размерности 256. Далее этот вектор поступает в классификационную часть модели:

1. Полносвязный слой из 256 нейронов («ReLU»), «Dropout»;
2. Полносвязный слой из 128 нейронов («ReLU»);
3. Выходной слой из одного нейрона с сигмоидной активацией.

Классификатор предсказывает вероятность того, что пара входных изображений принадлежит одному пользователю.

Модель обучалась с использованием оптимизатора Adam. Данный выбор обусловлен его эффективностью в задачах метрического обучения и способностью адаптировать скорость обучения для разреженных признаков скелетизированных изображений. Начальная скорость обучения (learning rate) выбиралась эмпирическим путем и составляла порядка 10^{-3}. В процессе обучения применялось экспоненциальное снижение скорости для более точной

настройки весов на финальных этапах. Веса инициализировались случайным образом (обучение с нуля), без использования предобученных на других задачах моделей, что позволяет сети максимально адаптироваться к специфике биометрических шаблонов.

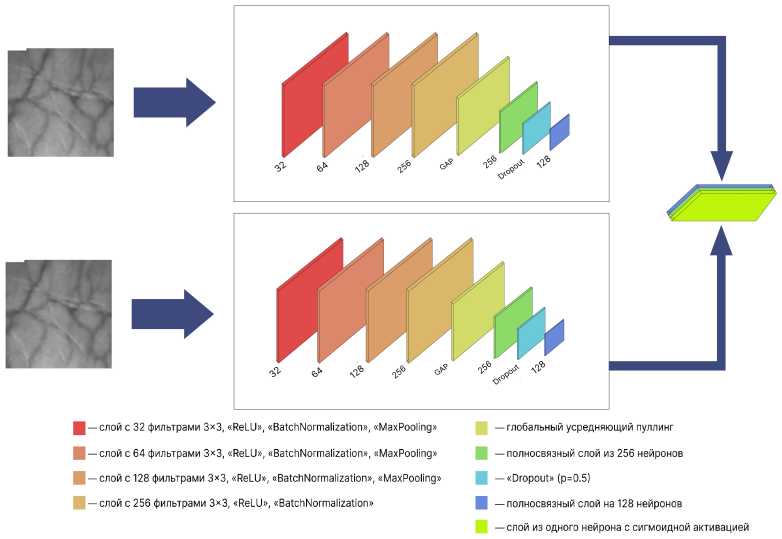

Рис.4 Архитектура нейросети

6. Модуль квантования и гомоморфного шифрования признаков с использованием открытого ключа. Основная задача данного этапа – обеспечение конфиденциальности биометрических данных посредством гомоморфного шифрования, реализуемого в асимметричной криптографической модели.

На первом этапе выполняется квантование элементов признакового вектора до целочисленного диапазона, совместимого с используемой гомоморфной схемой. Квантование осуществляется по линейному правилу с предварительной нормализацией значений к заданному диапазону. Это позволяет минимизировать искажения и сохранить структуру признаков в пределах допустимой точности. Глубина квантования может быть 8, 12 или 16 бит.

Для задач машинного обучения наиболее применимы схемы гомоморфного шифрования, поддерживающие операции над целыми числами. Это связано с тем, что признаки моделей могут быть приведены к целочисленному виду с помощью квантования, после

чего допускается выполнение линейной и сверточной арифметики в зашифрованном виде. В связи с этим, особый интерес для применения в защищенных биометрических системах представляет подход, реализованный в «Concrete ML», сочетающий возможность обработки тензоров, совместимость с популярными моделями и поддержание баланса между производительностью и защищенностью данных. Применение подобных библиотек позволяет выстраивать архитектуры, в которых конфиденциальность биометрических признаков обеспечивается на всем протяжении жизненного цикла данных – от извлечения до сравнения.

Далее применяется асимметричное шифрование квантованного вектора, основанное на схеме FHE (полное гомоморфное шифрование), которая является реализацией TFHE с поддержкой операций над тензорами, с использованием открытого ключа, сформированного в рамках асимметричной схемы гомоморфного шифрования.

В асимметричном шифровании (включая FHE):

Секретный ключ – используется для расшифровки. Хранится только у владельца, открытый ключ – используется для шифрования данных.

В FHE открытый ключ устроен так, что позволяет не только шифровать, но и производить над шифртекстом вычисления (сложение, умножение) без необходимости расшифровки. После шифрования каждый элемент признакового вектора преобразуется в соответствующий шифртекст.

7. Блок сравнения с эталоном и принятия решения сверточной моделью. После получения зашифрованного признакового вектора производится процесс сравнения с эталонным шаблоном, а также принятие решения о соответствии. В данной архитектуре используется заранее обученная сверточная нейросеть с сиамской структурой, адаптированная для обработки признаков в гомоморфно зашифрованной форме. Хранение эталонных шаблонов осуществляется в зашифрованном виде с использованием той же схемы гомоморфного шифрования. Все операции сравнения проводятся исключительно в зашифрованной области, без раскрытия признаков как на этапе загрузки, так и в процессе вычислений.

На первом этапе извлекается соответствующий эталон, привязанный к идентификатору пользователя. Вместо вычитания, два признаковых вектора – полученный в текущей сессии и эталонный – объединяются с помощью операции конкатенации. В результате

формируется вектор длины 256, содержащий полную информацию о паре сравниваемых признаков.

Конкатенированный вектор подается на классификационный блок сверточной нейросети, реализующий оценку вероятности соответствия. Сиамская архитектура модели позволяет обрабатывать пары признаков и выявлять скрытые взаимосвязи между ними. В рамках реализации модель была предварительно обучена на обширной выборке положительных и отрицательных пар изображений ладоней, благодаря чему достигнуты низкие значения ошибок распознавания.

Система использует TFHE-подход с Table Lookup для реализации полного цикла нейросетевых вычислений в зашифрованном виде, включая конкатенацию (как тривиальную операцию), линейные слои (через умножение/сложение) и нелинейные активации (через табличные функции или полиномиальные аппроксимации).

Все операции выполняются в зашифрованной форме, сверточная нейросеть функционирует над гомоморфно зашифрованными данными, не раскрывая признаки ни на одном этапе обработки. Результатом работы модели является значение вероятности совпадения. При превышении порога считается, что аутентификация успешно подтверждена.

8. Описание датасета. Для проведения эксперимента был собран датасет из изображений датасетов CASIA-MS-PalmprintV1 [29] и Tongji Contactless Palmvein Dataset (изображения ладоней 300 различных персон).

Датасет CASIA – это эталонная база данных для тестирования многоспектральных биометрических систем. Содержит изображения ладоней обеих рук 100 различных персон в 6 спектральных диапазонах (видимый спектр, 460, 530, 700, 850 и 940 нм). Сбор данных датасета проводился в две сессии, временной интервал между которыми составлял более одного месяца, что позволяет тестировать алгоритмы на устойчивость к временным изменениям. В рамках каждой сессии делалось по 3 образца, между которыми допускались небольшие изменения в положении руки для увеличения внутриклассового разнообразия. Таким образом, датасет содержит 7200 полутоновых изображений размером 576 ×768 пикселей в формате JPEG. При сборке образцов была использована специально разработанная бесконтактная многоспектральная камера (без фиксирующих штырей), которая позволяет варьировать положение руки для имитации

реальных условий использования. Кроме того, датасет имеет четкую структуру именования файлов.

Tongji Contactless Palmvein Dataset – это крупномасштабная публичная база данных изображений ладонных вен. Содержит изображения ладоней обеих рук 300 персон (192 мужчины и 108 женщин), полученные с помощью ближнего инфракрасного (NIR) излучения. Сбор данных датасета проводился в две сессии, временной интервал между которыми 61 день, что позволяет тестировать алгоритмы на устойчивость к временным изменениям (возрастным или физиологическим). В рамках каждой сессии делалось по 10 снимков каждой ладони, между которыми допускались небольшие изменения в положении руки для увеличения внутриклассового разнообразия. Таким образом, датасет содержит 12000 полутоновых изображений в формате JPEG размером 600 ×800 пикселей.

Целью эксперимента является оценка эффективности алгоритма аутентификации, поэтому датасет собран таким образом, чтобы исключить ошибки выделения ROI и явные дефекты изображений. Объединенный датасет изображений включает 326 пользователей, по 6 изображений каждой ладони на каждого пользователя и состоит из 1956×2 = 3912 изображений. Для формирования тестовой выборки случайным образом выделены 50 пользователей (600 изображений), оставшийся датасет (3312 изображений) был разделен для обучения и валидации в соотношении 80% и 20% соответственно.

9. Проведение эксперимента. На один из каналов подается ROI, а на второй – вектор признаков пользователя, зарегистрированного в базе данных. Такой способ сравнения позволяет, в процессе функционирования системы, сократить время отклика нейросети почти в два раза. Из каждого изображения формировались пары:

– положительные – изображения одной и той же ладони;

– отрицательные – изображения ладоней разных пользователей.

Таким образом, обучающая выборка включала равное количество положительных и отрицательных пар, что обеспечило сбалансированность классов.

Обучение проводилось с использованием функции потерь бинарной кроссэнтропии. В качестве оптимизатора использовался алгоритм Adam с параметрами по умолчанию: beta_1 = 0.9 (коэффициент для первого момента), beta_2 = 0.999 (коэффициент для второго момента), weight_decay (L2-регуляризация) – kernel_regularizer=l2(1e-4). Версия фреймворка TensorFlow 2.18.

Используется функция train_test_split из scikit-learn с параметром test_size=0.2. random_state=42. Обучение осуществлялось на GPU с автоматическим сохранением лучших весов по валидационной выборке. Размер батча составлял 32, обучение велось в течение 35 эпох.

Для тестирования алгоритма использован указанный выше датасет. Эксперименты проводились по следующему сценарию. На вход подавалось по очереди одно из 12 изображений каждого пользователя, формировались по 10 положительных и отрицательных пар, что позволило имитировать 500 «подходов» пользователей к БИК-камере без учета аугментации.

Для количественной оценки эффективности разработанной СБА выбраны ключевые показатели:

– общая точность (accuracy)

$$accuracy = \frac{TP+TN}{TP+TN+FP+FN};$$

где TN – количество правильных отказов пользователям, которых нет в базе, FP – количество ошибочных предоставлений доступа пользователям, которых нет в базе, TP – количество правильных предоставлений доступа пользователям, которые есть в базе, FN – количество ошибочных отказов в доступе пользователям, которые есть в базе:

– уровень ложных допусков (FAR)

– $FAR = \frac{FP}{FP+TN}$;

– уровень ложных отказов (FRR)

– $FRR = \frac{FN}{TP+FN}$;

– EER – показатель, определяющий баланс FAR и FRR;

– F1-мера, характеризующая баланс между ложноположительными и ложноотрицательными ошибками классификатора:

$$F_1 = 2 \times \frac{Precision \times Recall}{Precision+Recall},$$

где:

$$Precision = \frac{TP}{TP+FP}, Recall = \frac{TP}{TP+FN},$$

– площадь под ROC-кривой (AUC).

Модель оценивалась при различных порогах принятия решения, для чего построен график, отображающий FAR, FRR и EER от порогового значения (Рис. 5).

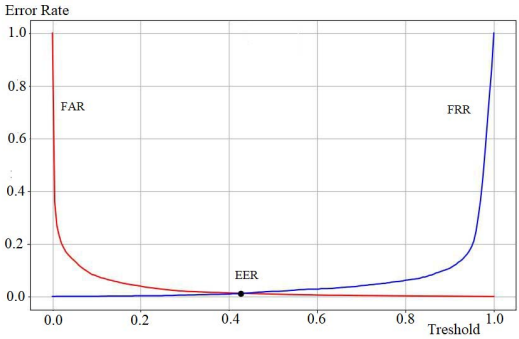

Рис. 5. Зависимость FAR и FRR от порогового значения (Treshold)

Значения показателей оценки эффективности биометрической системы аутентификации были получены при пороге 0,52, который был подобран эмпирически на валидационной выборке, и представлены в таблице 1.

Таблица 1. Показатели эффективности системы аутентификации

accuracy	FAR	FRR	F1	EER	AUC
98,2 %	0,67 %	1,38 %	98%	0,73 %	0,96

Для более подробной оценки качества классификации дополнительно была построена ROC-кривая, отражающая зависимость между долей истинно положительных срабатываний («True Positive Rate») и ложноположительных срабатываний («False Positive Rate»). Полученная кривая продемонстрировала стремительный рост TPR при низких значениях FPR, что свидетельствует о высокой дискриминационной способности модели. Значение площади под ROC-кривой (AUC) составило 0,96, что подтверждает высокую точность работы модели на всей области значений порога. ROC-кривая представлена на рисунке 6.

Время обработки биометрических данных с момента снятия изображения с камеры до шифрования данных составляет 0,06 с. Время, затраченное на шифрование, квантование и классификацию колеблется в зависимости от глубины квантования: для 16 бит – 2,0-2,2 с., при 8-

битном квантовании – 0,9-1,2 с. При этом снижение глубины квантования до 8 бит не привело к значимым потерям точности. Исследование проводилось на стандартной рабочей станции с процессором Intel Core i5 и 16 ГБ оперативной памяти без использования графических ускорителей.

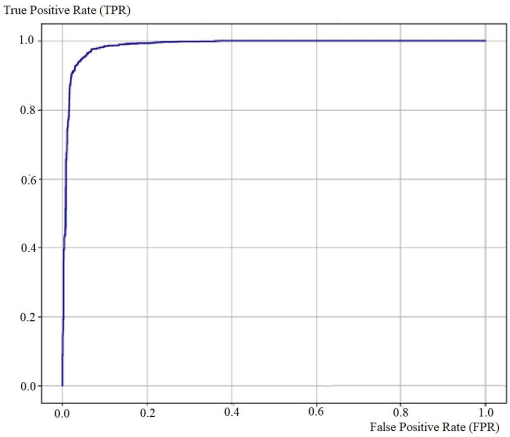

Рис. 6. ROC-кривая

Для оценки устойчивости СБА были проведены дополнительные эксперименты, направленные на изучение ее поведения при наличии искажений во входных данных, а также при варьировании параметров шифрования. Исследование проводилось на той же выборке, что и в основном эксперименте, с применением искусственно модифицированных изображений и измененных конфигураций квантования.

В качестве факторов искажения входных изображений рассматривались:

1. Смещение области ROI в пределах ±5 пикселей по осям x и y;
2. Поворот изображения на ±5 и ±10 градусов;
3. Добавление гауссовского шума с дисперсией 0.01;
4. Изменение контрастности (CLAHE с различными параметрами);
5. Небольшие масштабные искажения ROI (±10%).

Внесение в базу данных искаженных изображений позволило увеличить число «подходов» до 5000.

Показатели точности при введении искажений снижались незначительно. Наибольшее влияние оказывало смещение ROI:

при смещении на 5 пикселей accuracy снижалась на 1,3 %, а FRR возрастала до 2,4 %. При других видах искажений снижение точности не превышало 1 %. Это свидетельствует об устойчивости модели к небольшим ошибкам локализации и колебаниям условий съемки.

В таблице 2 приведены параметры точности (accuracy) и средняя ошибка аутентификации (EER) предложенной СБА с аналогичными системами, представленными в обзоре.

Таблица 2. Сравнение результатов с работы СБА по рисунку вен ладони

Источник	год	модель	dataset	Accuracy (%)	EER(%)
[4]	2021	CNN	Casia	99,4	0,0683
[5]	2021	CNN	Casia, PUT	99,83	0,0556
[6]	2021	GAN+ CNN	Casia, PUT	98 98,82	нет данных
[7]	2021	CNN	MS-PolyU	94,65	нет данных
[8]	2023	CNN	PolyU, Tongji	нет данных	0,28 1,07
[9]	2023	GCNLE+ Attention	PolyU, VERA	98,82 98,27	нет данных
[10]	2023	LST+GAN	PolyU, Tongji	93,6 88,7	нет данных
[11]	2023	ResNet-32, SingleNet	Cassia, PolyU	99,2 100	нет данных
[12]	2024	Deep Autoencoder + Siamese network	Tecnocampus Hand Image	98,79	нет данных
Предложенный	2025	Siamese network	Cassia + Tongji	98,2	0,73

Сравнение результатов показывает, что разработанная СБА уступает по точности системам, разработанным в [4 – 6, 11] из-за ограниченности в вычислительных ресурсах и необходимости применения легковесной нейронной сети, но при этом обеспечена защищенная обработка биометрических данных и возможность использования для встраиваемых систем, результаты [7 – 10] сопоставимы по точности классификации с предложенной СБА. В работе [12] представлена биометрическая система, являющаяся

наиболее близким прототипом, реализованная на одноплатном компьютере Raspberry Pi 3 Model B с CPU. Проведем сравнительный анализ полученных результатов разработанной СБА и прототипа [12] в таблице 3.

Таблица 3 Сравнение параметров с известным подобным решением

Параметр для сравнения	[12]	Предложенный
Обработка биометрических данных	Применение глубокого автоэнкодера для предварительной обработки	Предварительная обработка, выделение рисунка вен
Время обработки биометрических данных	Raspberry Pi 3 – 1,8 с. Desktop GPU -0,36 с.	Raspberry Pi 5 – 0,18 с. Desktop без GPU -0,06 с.
Классификация	Сиамская нейронная сеть	Сиамская нейронная сеть
Время классификации	Raspberry Pi 3– 3,8 с. Desktop GPU – 0,001 с.	Raspberry Pi 5– 0,21 с. Desktop без GPU -0,07 с.
Accuracy	98,79%	98,2%
EER	Нет данных	0,73%
Защита биометрических данных	отсутствует	Гомоморфное шифрование
Время шифрования		Raspberry Pi 5 – 3,62 с. Desktop без GPU - 1,2 с.

Сравнивая разработанную систему с прототипом, можно сказать, предложенная СБА не уступает [12], как по точности, так и по времени обработки, но при этом обеспечивает защищенную обработку данных.

10. Заключение. Разработанная система биометрической аутентификации демонстрирует практическую реализуемость защищённой биометрической аутентификации с применением гомоморфного шифрования. Точность классификации составляет 98,2%, время отклика составляет 1,2 с. при реализации на ПК и 4 с. при реализации на Raspberry Pi 5, что соответствует постановке задачи. Результаты экспериментов подтверждают, что даже при варьировании параметров и наличии искажений входных данных разработанная архитектура сохраняет стабильное поведение, обеспечивая приемлемый уровень ошибок и устойчивость в условиях неполной достоверности входной информации. Это позволяет адаптировать ее под различные

сценарии эксплуатации – от встроенных систем с жесткими ограничениями по вычислительным ресурсам до облачных платформ с повышенными требованиями к точности. Сокращение времени обработки может быть обеспечено как использованием специализированных вычислительных ускорителей (GPU, TPU, FPGA), так и применением других библиотек, поддерживающих гомоморфные вычисления, менее требовательных к вычислительным ресурсам.

Литература

1. Ryu R., Yeom S., Herbert D., Dermoudy J. The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction // ICT Express. 2023. vol. 9. no. 6. pp. 1183–1197. DOI: 10.1016/j.icte.2023.04.003
2. Boshoff D., Hancke G.P. A Classifications Framework for Continuous Biometric Authentication (2018–2024) // Computers & Security. 2024. vol. 150. 104285 p.
3. Nayar G.R., Thomas T. Partial palm vein based biometric authentication // Journal of Information Security and Applications. 2023. vol. 72. 103390 p.
4. Obayya M.I., El-Ghandour M., Alrowais F. Contactless Palm Vein Authentication Using Deep Learning With Bayesian Optimization // IEEE Access. 2020. vol. 9. pp. 1940–1957. DOI: 10.1109/ACCESS.2020.3045424.
5. Chen Y.-Y., Hsia C.-H., Chen P.-H. Contactless Multispectral Palm-Vein Recognition With Lightweight Convolutional Neural Network // IEEE Access. 2021. vol. 9. pp. 149796–149806. DOI: 10.1109/ACCESS.2021.3124631.
6. Qin H., El-Yacoubi M.A., Li Y., Liu C. Multi-Scale and Multi-Direction GAN for CNN-Based Single Palm-Vein Identification // IEEE Transactions on Information Forensics and Security. 2021. vol. 16. pp. 2652–2666. DOI: 10.1109/TIFS.2021.3059340.
7. Kaddoun S.S., Aberni Y., Boubchir L., Raddadi M., Daachi B. Convolutional Neural Algorithm for Palm Vein Recognition using ZFNet Architecture // Proceedings of the 4th International Conference on Bio-Engineering for Smart Technologies (BioSMART). 2021. pp. 1–4. DOI: 10.1109/BioSMART54244.2021.9677799.
8. Ma Y., et al. Focal Contrastive Learning for Palm Vein Authentication // IEEE Transactions on Instrumentation and Measurement. 2023. vol. 72. pp. 1–15. DOI: 10.1109/TIM.2023.3304689.
9. Qin H., Gong C., Li Y., Gao X., El-Yacoubi M.A. Label Enhancement-Based Multiscale Transformer for Palm-Vein Recognition // IEEE Transactions on Instrumentation and Measurement. 2023. vol. 72. pp. 1–17. DOI: 10.1109/TIM.2023.3261909.
10. Li Y., Ruan S., Qin H., Deng S., El-Yacoubi M.A. Transformer Based Defense GAN Against Palm-Vein Adversarial Attacks // IEEE Transactions on Information Forensics and Security. 2023. vol. 18. pp. 1509–1523. DOI: 10.1109/TIFS.2023.3243782.
11. Hernandez-Garcia R., Salazar-Jurado E.H., Barrientos R.J., Castro F.M., Ramos-Cozar J., Guil N. From Synthetic Data to Real Palm Vein Identification: a Fine-Tuning Approach // Proceedings of the IEEE 13th International Conference on Pattern Recognition Systems (ICPRS). 2023. pp. 1–7. DOI: 10.1109/ICPRS58416.2023.10179042.
12. Nunes M., Viegas E.K., Santin A.O. Towards a Feasible Palm Vein Verification Scheme Using Deep Autoencoder and Siamese Networks // 2024 International Conference on Machine Learning and Applications (ICMLA). 2024. pp. 483–489. DOI: 10.1109/ICMLA61862.2024.00071.
13. Manikandan V.M. Chapter 11 - A secure biometric authentication system for smart environment using reversible data hiding through encryption scheme // Machine Learning for Biometrics Concepts, Algorithms and Applications Cognitive Data Science in Sustainable Computing. 2022. pp. 201–216.

14. Zeng L., Shen P., Zhu X., Tian X., Chen C. A review of privacy-preserving biometric identification and authentication protocols // Computers & Security. 2025. vol. 150. 104309 p. DOI: 10.1016/j.cose.2024.104309.
15. Adil M., Farouk A., Ali A., Song H., Jin Z. Securing Tomorrow of Next-Generation Technologies with Biometrics, State-of-The-Art Techniques, Open Challenges, and Future Research Directions // Computer Science Review. 2025. vol. 57. 100750 p.
16. Melzi P., Rathgeb C., Tolosana R., Vera-Rodriguez R., Busch C. An Overview of Privacy-Enhancing Technologies in Biometric Recognition // ACM Computing Surveys. 2024. 12 p. DOI: 10.1145/3664596.
17. Wang X., Xie Y., Shui D., Ge S. An improved biometric authentication and key agreement scheme based on fuzzy extractor for Wireless Body Area Networks // Journal of Information Security and Applications. 2025. vol. 91. 104047 p. DOI: 10.1016/j.jisa.2025.104047.
18. Srinivas P.V.V.S, Yadavalli N., DurgaV., Kumar K., Raju P. Enhanced biometric template protection schemes using distance based fuzzy extractor // Computers & Security. 2025. vol. 157. 104573 p.
19. ISO/IEC 24745 / Information security, cybersecurity and privacy protection – Biometric information protection // ISO/IEC. 2022. 63 p.
20. Morampudi M.K., Prasad M.V.N.K., Verma M., Raju U.S.N. Secure and verifiable iris authentication system using fully homomorphic encryption // Computers & Electrical Engineering. 2021. vol. 89. 106924 p. DOI: 10.1016/ j.compeleceng.2020.106924.
21. Wu B., Zheng S., Dai P., Chen J., Yao Y. Searchable face recognition authentication based on homomorphic encryption // Journal of Information Security and Applications. 2025. vol. 94. 104208 p. DOI: 10.1016/j.jisa.2025.104208.
22. Wu L., Wang X.A., Liu J., Su Y., Zheng T., Liu W., Lei H., Tang D., Cao Y., Zhang J. Homomorphic Encryption for Machine Learning Applications with CKKS Algorithms: A Survey of Developments and Applications // Computers, Materials @ Continua. 2025. vol. 85. no. 1. DOI: 10.32604/cmc.2025.064346.
23. Wang H., Liu W., Wang X.A., Jiang W., Liu J., Yang X., Zhao W., Zheng K. Privacy-enhanced facial recognition for IoT based on homomorphic encryption // Internet of Things. 2025. vol. 34. 101757 p. DOI: 10.1016/j.iot.2025.101757.
24. Sumalatha U., Prakasha K.K., Prabhu S., Nayak V.C. A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection // IEEE Access. 2024. vol. 12. pp. 64300–64334. DOI: 10.1109/ACCESS.2024.3395417.
25. Hemis M., Kheddar H., Bourouis S., Saleem N. Deep learning techniques for hand vein biometrics: A comprehensive review // Information Fusion. 2025. vol. 114. 102716 p. DOI: 10.1016/j.inffus.2024.102716.
26. Kurbatova E., Kharina N., Zemtsov A., Plyaskin S. Investigating Palm Vein Pattern Recognition Methods // Proceedings of the 24th International Conference on Digital Signal Processing and its Applications (DSPA). 2022. pp. 1–5. DOI: 10.1109/DSPA53304.2022.9790783.
27. Boudaoud B.L., Solaiman B., Tari A. A modified ZS thinning algorithm by a hybrid approach // The Visual Computer. 2018. vol. 34. pp. 689–706. DOI: 10.1007/s00371-17-1407-4.
28. Прозоров Д.Е., Земцов А.В. Применение легковесной сиамской нейросети для формирования вектора признаков в системе васкулярной аутентификации // Компьютерная оптика. 2023. Т. 47. №3. С. 433–441.
29. Note on CASIA Palmprint Database // CBSR. URL: http://www.cbsr.ia.ac.cn/english/ Palmprint%20Databases.asp.

Харина Наталья Леонидовна — канд. техн. наук, доцент, доцент кафедры радиоэлектронных средств, ВятГУ. Область научных интересов: компьютерное зрение, биометрическая аутентификация, искусственный интеллект в прикладных решениях, моделирование процессов различной природы с применением теории условных Марковских процессов. Число научных публикаций — 106. harina@vyatsu.ru; ул. Московская, д. 36, г. Киров, 610000, РФ; моб.т. +7(909)140-4746.

Долженкова Мария Львовна — канд. техн. наук, доцент, зав. кафедрой электронно-вычислительных машин, ВятГУ. Область научных интересов: системы поддержки принятия решений на знаниях, технологии глубокого обучения, искусственный интеллект в прикладных решениях. Число научных публикаций — 59. maryd@vyatsu.ru; ул. Московская, д. 36, г. Киров, 610000, РФ; моб.т. +7(912)825-2061.

Иминова Зарина Бахтияржановна — студент 4 курса, ВятГУ. Область научных интересов: компьютерное зрение, биометрическая аутентификация. stud143619@vyatsu.ru; ул. Московская, д. 36, г. Киров, 610000, РФ; моб.т. +7(922)662-7545.

DOI 10.15622/ia.25.3.10

N. HARINA, M. DOLZHENKOVA, Z. IMINOVA

SECURE BIOMETRIC AUTHENTICATION SYSTEM FOR EMBEDDED SYSTEMS WITH LIMITED COMPUTING RESOURCES

Harina N., Dolzhenkova M., Iminova Z. **Secure Biometric Authentication System for Embedded Systems with Limited Computing Resources.**

Abstract. Biometric authentication technologies such as face, fingerprint, iris, and palm vein recognition are currently widely used in banking applications, medical systems, access control systems, and government information resources. The use of such technologies must be accompanied by measures to protect biometric information during processing and storage, especially in the face of the growing number of targeted attacks on personal data. One promising approach to ensuring the security of biometric information is the use of homomorphic encryption. The paper presents an autonomous secure biometric authentication system based on the user's palm vein patterns in the near infrared spectrum for embedded solutions implemented using privacy-preserving technology to protect biometric data. Studies have shown the practical feasibility of a biometric authentication system using a lightweight Siamese neural network to extract a feature vector and homomorphic encryption to ensure confidentiality on processors with limited computing resources based on single-board computers such as Raspberry Pi. Resistance to distortion, including rotations, noise, displacements, and varying encryption parameters, has been confirmed. The performance of the developed system was evaluated on a combined dataset consisting of images from the CASIA-MS-PalmprintV1 and Tongji Contactless Palmvein datasets, yielding the following results: classification accuracy 98.2%, EER 0.73%, AUC 0.96, and processing time 1.2 seconds, which meet the requirements for such systems. Analysis of the results shows that the developed system is inferior in accuracy to client-server solutions based on heavyweight convolutional neural networks due to limited computing resources and the consequent need for a lightweight neural network, but at the same time it provides secure biometric data processing while maintaining an acceptable response time. Reducing the processing time when implemented on single-board computers can be achieved by using both specialized computing accelerators and by employing other libraries that support homomorphic computations and are less demanding on computing resources.

Keywords: biometric authentication, image processing, convolutional neural network, Siamese neural network, privacy-preserving biometric processing, homomorphic encryption.

References

1. Ryu R., Yeom S., Herbert D., Dermoudy J. The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. ICT Express. 2023. vol. 9. no. 6. pp. 1183–1197. DOI: 10.1016/j.icte.2023.04.003
2. Boshoff D., Hancke G.P. A Classifications Framework for Continuous Biometric Authentication (2018–2024). Computers & Security. 2024. vol. 150. 104285 p.
3. Nayar G.R., Thomas T. Partial palm vein based biometric authentication. Journal of Information Security and Applications. 2023. vol. 72. 103390 p.
4. Obayya M.I., El-Ghandour M., Alrowais F. Contactless Palm Vein Authentication Using Deep Learning With Bayesian Optimization. IEEE Access. 2020. vol. 9. pp. 1940–1957. DOI: 10.1109/ACCESS.2020.3045424.

5. Chen Y.-Y., Hsia C.-H., Chen P.-H. Contactless Multispectral Palm-Vein Recognition With Lightweight Convolutional Neural Network. IEEE Access. 2021. vol. 9. pp. 149796–149806. DOI: 10.1109/ACCESS.2021.3124631.
6. Qin H., El-Yacoubi M.A., Li Y., Liu C. Multi-Scale and Multi-Direction GAN for CNN-Based Single Palm-Vein Identification. IEEE Transactions on Information Forensics and Security. 2021. vol. 16. pp. 2652–2666. DOI: 10.1109/TIFS.2021.3059340.
7. Kaddoun S.S., Aberni Y., Boubchir L., Raddadi M., Daachi B. Convolutional Neural Algorithm for Palm Vein Recognition using ZFNet Architecture. Proceedings of the 4th International Conference on Bio-Engineering for Smart Technologies (BioSMART). 2021. pp. 1–4. DOI: 10.1109/BioSMART54244.2021.9677799.
8. Ma Y., et al. Focal Contrastive Learning for Palm Vein Authentication. IEEE Transactions on Instrumentation and Measurement. 2023. vol. 72. pp. 1–15. DOI: 10.1109/TIM.2023.3304689.
9. Qin H., Gong C., Li Y., Gao X., El-Yacoubi M.A. Label Enhancement-Based Multiscale Transformer for Palm-Vein Recognition. IEEE Transactions on Instrumentation and Measurement. 2023. vol. 72. pp. 1–17. DOI: 10.1109/TIM.2023.3261909.
10. Li Y., Ruan S., Qin H., Deng S., El-Yacoubi M.A. Transformer Based Defense GAN Against Palm-Vein Adversarial Attacks. IEEE Transactions on Information Forensics and Security. 2023. vol. 18. pp. 1509–1523. DOI: 10.1109/TIFS.2023.3243782.
11. Hernandez-Garcia R., Salazar-Jurado E.H., Barrientos R.J., Castro F.M., Ramos-Cozar J., Guil N. From Synthetic Data to Real Palm Vein Identification: a Fine-Tuning Approach. Proceedings of the IEEE 13th International Conference on Pattern Recognition Systems (ICPRS). 2023. pp. 1–7. DOI: 10.1109/ICPRS58416.2023.10179042.
12. Nunes M., Viegas E.K., Santin A.O. Towards a Feasible Palm Vein Verification Scheme Using Deep Autoencoder and Siamese Networks. 2024 International Conference on Machine Learning and Applications (ICMLA). 2024. pp. 483–489. DOI: 10.1109/ICMLA61862.2024.00071.
13. Manikandan V.M. Chapter 11 - A secure biometric authentication system for smart environment using reversible data hiding through encryption scheme. Machine Learning for Biometrics Concepts, Algorithms and Applications Cognitive Data Science in Sustainable Computing. 2022. pp. 201–216.
14. Zeng L., Shen P., Zhu X., Tian X., Chen C. A review of privacy-preserving biometric identification and authentication protocols. Computers & Security. 2025. vol. 150. 104309 p. DOI: 10.1016/j.cose.2024.104309.
15. Adil M., Farouk A., Ali A., Song H., Jin Z. Securing Tomorrow of Next-Generation Technologies with Biometrics, State-of-The-Art Techniques, Open Challenges, and Future Research Directions. Computer Science Review. 2025. vol. 57. 100750 p.
16. Melzi P., Rathgeb C., Tolosana R., Vera-Rodriguez R., Busch C. An Overview of Privacy-Enhancing Technologies in Biometric Recognition. ACM Computing Surveys. 2024. 12 p. DOI: 10.1145/3664596.
17. Wang X., Xie Y., Shui D., Ge S. An improved biometric authentication and key agreement scheme based on fuzzy extractor for Wireless Body Area Networks. Journal of Information Security and Applications. 2025. vol. 91. 104047 p. DOI: 10.1016/j.jisa.2025.104047.
18. Srinivas P.V.V.S, Yadavalli N., DurgaV., Kumar K., Raju P. Enhanced biometric template protection schemes using distance based fuzzy extractor. Computers & Security. 2025. vol. 157. 104573 p.
19. ISO.IEC 24745. Information security, cybersecurity and privacy protection – Biometric information protection. ISO.IEC. 2022. 63 p.

20. Morampudi M.K., Prasad M.V.N.K., Verma M., Raju U.S.N. Secure and verifiable iris authentication system using fully homomorphic encryption. Computers & Electrical Engineering. 2021. vol. 89. 106924 p. DOI: 10.1016/j.compeleceng.2020.106924.
21. Wu B., Zheng S., Dai P., Chen J., Yao Y. Searchable face recognition authentication based on homomorphic encryption. Journal of Information Security and Applications. 2025. vol. 94. 104208 p. DOI: 10.1016/j.jisa.2025.104208.
22. Wu L., Wang X.A., Liu J., Su Y., Zheng T., Liu W., Lei H., Tang D., Cao Y., Zhang J. Homomorphic Encryption for Machine Learning Applications with CKKS Algorithms: A Survey of Developments and Applications. Computers, Materials @ Continua. 2025. vol. 85. no. 1. DOI: 10.32604/cmc.2025.064346.
23. Wang H., Liu W., Wang X.A., Jiang W., Liu J., Yang X., Zhao W., Zheng K. Privacy-enhanced facial recognition for IoT based on homomorphic encryption. Internet of Things. 2025. vol. 34. 101757 p. DOI: 10.1016/j.iot.2025.101757.
24. Sumalatha U., Prakasha K.K., Prabhu S., Nayak V.C. A Comprehensive Review of Unimodal and Multimodal Fingerprint Biometric Authentication Systems: Fusion, Attacks, and Template Protection. IEEE Access. 2024. vol. 12. pp. 64300–64334. DOI: 10.1109/ACCESS.2024.3395417.
25. Hemis M., Kheddar H., Bourouis S., Saleem N. Deep learning techniques for hand vein biometrics: A comprehensive review. Information Fusion. 2025. vol. 114. 102716 p. DOI: 10.1016/j.inffus.2024.102716.
26. Kurbatova E., Kharina N., Zemtsov A., Plyaskin S. Investigating Palm Vein Pattern Recognition Methods. Proceedings of the 24th International Conference on Digital Signal Processing and its Applications (DSPA). 2022. pp. 1–5. DOI: 10.1109/DSPA53304.2022.9790783.
27. Boudaoud B.L., Solaiman B., Tari A. A modified ZS thinning algorithm by a hybrid approach. The Visual Computer. 2018. vol. 34. pp. 689–706. DOI: 10.1007/s00371-17-1407-4.
28. Prozorov D.E., Zemtsov A.V. [Application of a lightweight Siamese neural network to generate a feature vector in a vascular authentication system]. Kompyuternaya optika – Computer optics. 2023. vol. 47. no. 3. pp. 433–441. (In Russ.).
29. Note on CASIA Palmprint Database. CBSR. Available at: http://www.cbsr.ia.ac.cn/english/Palmprint%20Databases.asp

Harina Natalya — Ph.D., Associate professor, Docent, Department of Radio Electronic Devices, Federal State Budgetary Educational Institution of Higher Education "Vyatka State University" (VyatSU). Research interests: computer vision, biometric authentication, artificial intelligence in applied solutions, modeling of processes of various nature using the theory of conditional Markov processes. The number of publications — 106. harina@vyatsu.ru; 36, Moskovskaya St., 610000, Kirov, Russia; office phone: +7(909)140-4746.

Dolzhenkova Maria — Ph.D., Associate professor, Head of the Department, Department of Electronic Computing Machines, Federal State Budgetary Educational Institution of Higher Education "Vyatka State University" (VyatSU). Research interests: knowledge-based decision support systems, deep learning technologies, artificial intelligence in applied solutions. The number of publications — 59. maryd@vyatsu.ru; 36, Moskovskaya St., 610000, Kirov, Russia; office phone: +7(912)825-2061

Iminova Zarina — Student, Federal State Budgetary Educational Institution of Higher Education "Vyatka State University" (VyatSU). Research interests: computer vision, biometricauthentication. The number of publications — 0. stud143619@vyatsu.ru; 36, Moskovskaya St., 610000, Kirov, Russia; office phone: +7(922)662-7545.