

УДК 004.056.5

Шифр специальности ВАК: 2.3.6

С.Е. Штука, А.Е. Боршевников

Модификация нейросетевого алгоритма высоконадёжной биометрической аутентификации по радужной оболочке глаза

Актуальность. Рост числа систем, обрабатывающих конфиденциальные данные, требует механизмов аутентификации, устойчивых к компрометации хранимых эталонов. **Цель исследования.** Модификация нейросетевого алгоритма высоконадёжной биометрической аутентификации по радужной оболочке глаза, обеспечивающая восстановление криптографического ключа с точным побитовым совпадением. **Методы.** Свёрточная нейронная сеть для выделения области радужной оболочки, нормализация кадрированием, совместное обучение свёрточной модели для извлечения признаков и многослойного персептрона с использованием комбинированной функции потерь, включающей метрические слагаемые и два слагаемых, действующих непосредственно в битовом выходе модели; выбор рабочей точки по критерию допустимости; перебор в окрестности Хэмминга при проверке. **Научная новизна.** В отличие от известных схем, точное восстановление ключа достигается без вспомогательных данных и внешней коррекции ошибок, что позволяет хранить только хэш ключа. **Результаты.** Для 100 зарегистрированных пользователей у экземпляров, допущенных к эксплуатации, доля истинного принятия составила 0,875 при нулевой вероятности ложного допуска на 8000 предъявлений «Чужих»; перебор в окрестности радиуса два бита снижает вероятность ошибки первого рода до 0,107, не изменяя вероятность ошибки второго рода. Отказ по обоим попыткам при точном совпадении ключа наблюдался у 1 пользователя из 100. Показано, что запас, обеспечиваемый на группе подбора порога, переносится на тестовую выборку лишь частично. **Практическая значимость.** Алгоритм применим в системах, где недопустимо хранение биометрических эталонов и криптографических ключей в открытом виде.

Ключевые слова: биометрическая аутентификация, радужная оболочка, сегментация изображений, нейронные сети, криптографический ключ, Triplet Loss, Center Loss, биометрическая криптография.

DOI: 10.21293/1818-0442-2026-29-2-148-159

Введение

Развитие цифровых сервисов и распределённых информационных систем требует повышения надёжности механизмов аутентификации пользователей. Данная задача особенно актуальна для систем, обрабатывающих конфиденциальные данные и критически важную информацию.

Используемые на практике парольные схемы аутентификации обладают рядом ограничений, связанных с возможностью компрометации учётных данных вследствие утечек баз данных, фишинга и человеческого фактора. Альтернативой служат биометрические технологии, использующие уникальные физиологические характеристики человека. Такой подход не требует от человека запоминания дополнительной информации и наличия дополнительных устройств [1]. Среди различных биометрических характеристик особый интерес представляет радужная оболочка глаза, отличающаяся высокой сложностью текстурного рисунка, значительной энтропией признаков и стабильностью во времени [1, 2]. Индивидуальность и неизменность радужной оболочки на протяжении жизни делают её перспективной основой для высоконадёжных систем аутентификации.

Целью настоящей работы является модификация нейросетевого алгоритма высоконадёжной биометрической аутентификации по радужной оболочке глаза, обеспечивающая точное побитовое восстановление криптографического ключа и, как следствие, возможность хранения только хэша ключа. Для достижения поставленной цели решались следующие задачи: сравнение архитектур сегментации в единых

условиях и выбор архитектуры для конвейера; выбор способа нормализации выделенной области; разработка функции потерь, обеспечивающей одновременно восстановление ключа «Своего» и удаление кодов «Чужих» от базы ключей; формирование процедуры выбора рабочей точки, гарантирующей нулевую оценку вероятности ошибки второго рода. Научная новизна работы состоит в переходе от порогового решения по расстоянию Хэмминга к решению по точному совпадению ключа без использования вспомогательных данных, а также во введении двух дополнительных членов функции потерь, действующих непосредственно в битовом выходе модели.

Основные понятия и критерии оценки

Согласно ГОСТ Р 52633.0–2006 [3], под высоконадёжной биометрической аутентификацией понимается биометрическая аутентификация с приемлемой вероятностью ошибок первого рода и гарантированно малой вероятностью ошибок второго рода, сопоставимой по своему значению с вероятностью случайного подбора кода неизвестного криптографического ключа при малом числе попыток подбора.

Высоконадёжная биометрическая аутентификация является частным случаем биометрической аутентификации и наследует её классическую архитектуру, включающую три последовательных ключевых этапа: предобработку данных, извлечение биометрических признаков и восстановление криптографического ключа. Поскольку в данной работе в качестве биометрической характеристики используется радужная оболочка глаза, исходные данные представляют собой изображения. Для изображений этап пре-

доработки, как правило, сводится к выделению целевой области (сегментации) и приведению её к стандартному виду (нормализации), что позволяет устранить вариативность, вызванную условиями съёмки, и подготовить данные к извлечению признаков.

Сегментация представляет собой классификацию пикселей исходного изображения на два класса: «радужная оболочка» и «фон» (склера, зрачок, веки, ресницы, блики). Результатом является бинарная маска, указывающая точное расположение радужки. В рамках нормализации выделенная область радужной оболочки приводится к стандартному виду для стабильной работы последующих этапов.

Качество решения каждой из задач определяет итоговые значения метрик. Для объективного сравнительного анализа различных подходов в научном сообществе используется устоявшийся набор стандартизированных показателей.

Точность сегментации оценивается с помощью F1-меры [4] и коэффициента Жаккара (Intersection over Union – IoU) [4], которые вычисляются как

$$F1 = \frac{2 \times TP}{2 \times TP + FP + FN}; \quad (1)$$

$$IoU = \frac{TP}{TP + FP + FN}, \quad (2)$$

где TP – количество элементов положительного класса, классифицированных верно, FP – количество элементов отрицательного класса, ошибочно отнесённых к положительному, FN – количество элементов положительного класса, ошибочно отнесённых к отрицательному. Также используются пиксельная точность (Accuracy), точность (Precision) и полнота (Recall)

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}; \quad (3)$$

$$Precision = \frac{TP}{TP + FP}; \quad (4)$$

$$Recall = \frac{TP}{TP + FN}, \quad (5)$$

где TN – количество элементов отрицательного класса, классифицированных верно. При оценке сегментации положительным классом считаются пиксели радужной оболочки, отрицательным – пиксели фона.

Качество извлечения признаков оценить напрямую невозможно, только через анализ качества аутентификации, которая характеризуется ошибками первого и второго рода. Метрики FAR (False Acceptance Rate, вероятность ошибки второго рода), FRR (False Rejection Rate, вероятность ошибки первого рода), GAR (Genuine Acceptance Rate, доля истинного принятия) вычисляются следующим образом [5]:

$$FAR = \frac{FP}{FP + TN}; \quad (6)$$

$$FRR = \frac{FN}{FN + TP}; \quad (7)$$

$$GAR = 1 - FRR. \quad (8)$$

В контексте аутентификации положительным классом считается множество легитимных пользова-

телей, отрицательным – множество незарегистрированных пользователей.

Обзор методов сегментации радужной оболочки

Сегментация является критически важным этапом, поскольку ошибки выделения области радужной оболочки непосредственно влияют на качество последующего извлечения признаков. Исторически первыми применялись граничные методы, направленные на выделение контуров объектов по резким изменениям интенсивности. Известны три основных подхода этой группы [6]: интегродифференциальный оператор Даугмана, максимизирующий производную от средней интенсивности вдоль кругового контура [7], преобразование Хафа для поиска окружностей и метод, основанный на анализе распределения граничных точек [8, 9]. Согласно приведённому сравнению, оператор Даугмана точнее остальных, но существенно медленнее: преобразование Хафа работает в 2,5 раза быстрее при меньшей точности, а анализ распределения граничных точек – почти в 6 раз быстрее при точности на уровне преобразования Хафа. Общим ограничением этой группы остаётся чувствительность к бликам и перекрытию радужной оболочки веками и ресницами.

Существенно более высокие показатели качества сегментации дают методы на основе свёрточных нейронных сетей (CNN). Архитектура U-Net, изначально предложенная для сегментации биомедицинских изображений [10], была применена к сегментации радужной оболочки [11] и стала основой для специализированных решений: замена обычных свёрток расширенными увеличивает рецептивное поле без потери разрешения [12], плотные соединения между слоями улучшают поток градиентов [13], остаточные блоки в сочетании с модулем ASPP обеспечивают многомасштабный анализ [14], а сокращение числа параметров до 148 тыс. позволяет работать при ограниченных вычислительных ресурсах почти без потери качества [15].

Отдельное направление образуют архитектуры на основе трансформеров и гибридные решения, в которых свёрточные слои выделяют локальные признаки, а трансформерные блоки учитывают глобальные зависимости [16–19]. Достигаемые ими значения F1-меры ниже, чем у лучших свёрточных решений, к тому же число параметров и требования к объёму размеченных данных существенно выше.

Сводное сопоставление классов методов приведено в табл. 1. Прямое сравнение опубликованных значений затруднено тем, что работы выполнены на разных наборах данных и с разной разметкой, поэтому в таблице приведены достигнутые в первоисточниках максимумы, а сопоставление проводится по классам, а не по отдельным моделям. Из него следует, что для рассматриваемой задачи предпочтительны U-Net-подобные свёрточные архитектуры: они дают наивысшие значения F1-меры при числе параметров, на порядок меньшем, чем у трансформеров, и не требуют столь большого объёма размеченных данных. Именно эта группа исследована далее.

Сопоставление классов методов сегментации и извлечения признаков

Класс методов	Этап	Преимущества	Ограничения	Результативность
Граничные	Сегментация	Не требуют обучения, низкая вычислительная сложность	Чувствительность к бликам и перекрытиям	Accuracy до 0,90 [6]
Свёрточные (U-Net и модификации)	Сегментация	Наивысшая точность, автоматическое выделение признаков	Требуют размеченных данных	F1 до 0,9914 [14]
Трансформерные и гибридные	Сегментация	Учёт глобальных зависимостей	Большое число параметров, высокие требования к объёму данных	Accuracy до 0,9958 [16], F1 до 0,9548 [17–19]
Статистические	Признаки	Простота реализации	Неустойчивость к изменению освещения	Зависит от классификатора
Спектральные	Признаки	Компактный бинарный код	Жёстко заданное преобразование, нет адаптации к данным	Зависит от классификатора
Нейросетевые	Признаки	Адаптация к набору данных, возможность дообучения	Требуют обучения и размеченных данных	Зависит от классификатора

Методы нормализации и извлечения признаков

После сегментации выполняется преобразование выделенной области, компенсирующее изменение размера зрачка и перекрытие радужной оболочки веками. Классическим подходом является нормализация по методу Даугмана – отображение области из декартовой системы координат в псевдополярную [7, 20]. Альтернатива состоит в кадрировании изображения по границам маски с приведением к фиксированному размеру. Выбор в пользу кадрирования сделан по результатам [21]: при прочих равных условиях нормализация по методу Даугмана дала вероятность ошибки первого рода 0,337 против 0,0714 при кадрировании. Причина в том, что кадрирование сохраняет исходные текстурные соотношения, тогда как переход в псевдополярные координаты требует интерполяции и вносит дополнительное сглаживание.

Извлечение признаков определяет дискриминативную способность системы; исторически сложились статистический, спектральный и нейросетевой подходы. Статистические методы работают с распределением интенсивностей пикселей: анализом гистограмм и моментами изображения [22]; они просты в реализации, но плохо устойчивы к изменению освещения. Спектральные методы анализируют изображение в частотной области: фильтры Габора, положенные в основу алгоритма IrisCode [7], и дискретное косинусное преобразование [23]. Общим свойством обеих групп является жёстко заданное преобразование, не адаптирующееся к конкретному набору данных.

Нейросетевые методы такой адаптацией обладают. Предобученные свёрточные сети в роли моделей для извлечения признаков показали высокую эффективность [24], гибридные подходы дополняют их предварительной фильтрацией круговыми фильтрами Габора [25], отдельное направление образуют сиамские сети, обучающиеся на парах изображений [26, 27].

Для настоящей работы выбраны предобученные свёрточные сети. Сиамские сети, несмотря на успешность в задачах идентификации, для высоконадёжной аутентификации не подходят принципиально: их обу-

чение сближает представления похожих изображений, а не привязывает представление к заданному эталонному выходу, поэтому формируемый код оказывается производным от биометрических данных, что противоречит требованию ГОСТ Р 52633.0–2006 [3] о недопустимости формирования ключа непосредственно из биометрии. Также не рассматривались сквозные автоэнкодеры и трансформерные преобразователи: они не допускают послойного контролируемого обучения, предусмотренного ГОСТ Р 52633.5–2011 [28].

Методы аутентификации по радужной оболочке глаза

Завершающий этап аутентификации может быть реализован классификацией признаков методами машинного обучения (случайный лес, k -ближайших соседей, метод опорных векторов и др.) [20] либо восстановлением криптографического ключа с последующей проверкой: по хэшу, что требует точного восстановления каждого бита, или путём сравнения по расстоянию Хэмминга [21]. Первый подход прост, но не позволяет получить криптографический ключ и не является высоконадёжным. Второй включает как нечёткие методы и коды коррекции ошибок, так и методы, которые регламентируются линейкой стандартов ГОСТ Р 52633: ключ должен иметь энтропию не менее 128 бит, не храниться в открытом виде и формироваться с использованием сертифицированных генераторов случайных чисел [3].

Стандарты допускают применение нейросетевых преобразователей «биометрия–код», в частности, многослойных персептронов [28].

Нечёткие методы и коды коррекции ошибок позволяют компенсировать вариабельность биометрических данных [29]. Однако такие методы требуют хранения вспомогательной информации (helper data), что снижает общую безопасность системы.

Схемы, восстанавливающие ключ точно, для радужной оболочки реализованы в ряде работ; их сопоставление с предлагаемым решением приведено в табл. 2. В [30] ключ длиной до 252 бит связывается с отменяемым шаблоном радужки по схеме нечёткого обязательства, что при нулевой оценке вероятности ложного допуска даёт вероятность ошибки первого

рода 0,07; вспомогательные данные при этом хранятся на смарт-карте. В [31] по изображению радужки и секретному ключу формируется открытый ключ, допускающий незащищённое хранение, при объёме восстанавливаемого секрета 65 бит и нулевой вероятности восстановления секрета по изображению другого человека. В [32] нечёткое обязательство дополнено кодами с малой плотностью проверок на чётность и отбором наиболее устойчивых битов шаблона. Наиболее близкой по постановке является работа [33], в которой нечёткий экстрактор обеспечивает 105 бит энтропии ключа при доле истинного принятия 0,92.

Общим для перечисленных схем является то, что точность восстановления ключа достигается за счёт вспомогательных данных, сохраняемых или публикуемых при регистрации, и внешней коррекции ошибок. Таким образом, задача побитового восстановления ключа без вспомогательных данных, при котором проверка сводится к сравнению хэшей, для радужной оболочки остаётся нерешённой; именно эта задача рассматривается в настоящей работе.

В исследовании [21] была продемонстрирована эффективность системы, совмещающей свёрточную сеть для извлечения признаков и MLP для восстановления ключа в рамках одной модели. При нормализации кадрирования и пороге сравнения по расстоянию Хэмминга, равном 32 из 256 бит, система до-

стигла вероятности ошибки первого рода 0,0714 при нулевой оценке вероятности ложного допуска. Однако такой подход имеет два существенных ограничения: во-первых, внутриклассовая вариативность признаков не позволяет добиться полного побитового восстановления ключей; во-вторых, аутентификация по порогу не позволяет использовать криптографическое хэширование и требует хранения ключей в открытом виде, что снижает безопасность.

В настоящей работе этот алгоритм взят за основу и модифицируется.

Предлагаемый алгоритм высоконадёжной аутентификации

В рамках данного исследования предложен и экспериментально оценён нейросетевой алгоритм, при проектировании которого исследована эффективность различных подходов к сегментации, нормализации, а также методов снижения внутриклассовой вариативности на этапах извлечения признаков и восстановления ключа. Тестирование проводилось на наборе данных CASIA-Iris-Thousand, который содержит 20000 изображений радужной оболочки от 1000 субъектов. Левые и правые глаза рассматривались как независимые биометрические объекты, что позволило сформировать выборку из 2000 классов по 10 образцов в каждом.

Общая структура алгоритма приведена на рис. 1.

Таблица 2

Сравнение решений по восстановлению криптографического ключа по радужной оболочке глаза*

Работа	Длина ключа, бит	Вспомогательные данные	Критерий принятия решения	Вероятность ошибки I рода	Вероятность ошибки II рода
[21]	256	Не требуются	Порог расстояния Хэмминга (32 бита)	0,071	0
[30]	до 252	Требуются	Точное совпадение после коррекции	0,070	0
[31]	65	Требуются	Точное совпадение после коррекции	0,104	0
[32]	Не приводится	Требуются	Точное совпадение после коррекции	Не приводится	Не приводится
[33]	105 (энтропия)	Требуются	Точное совпадение после коррекции	0,080	Не приводится
Настоящая работа	512	Не требуются	Точное побитовое совпадение	0,107	0

* Работы выполнены на разных наборах данных и по разным протоколам, поэтому сопоставление вероятностей ошибок носит ориентировочный характер. Строго сопоставимы столбцы «Вспомогательные данные» и «Критерий принятия решения». Для настоящей работы приведены показатели экземпляров, допущенных к эксплуатации; процедура допуска описана далее.

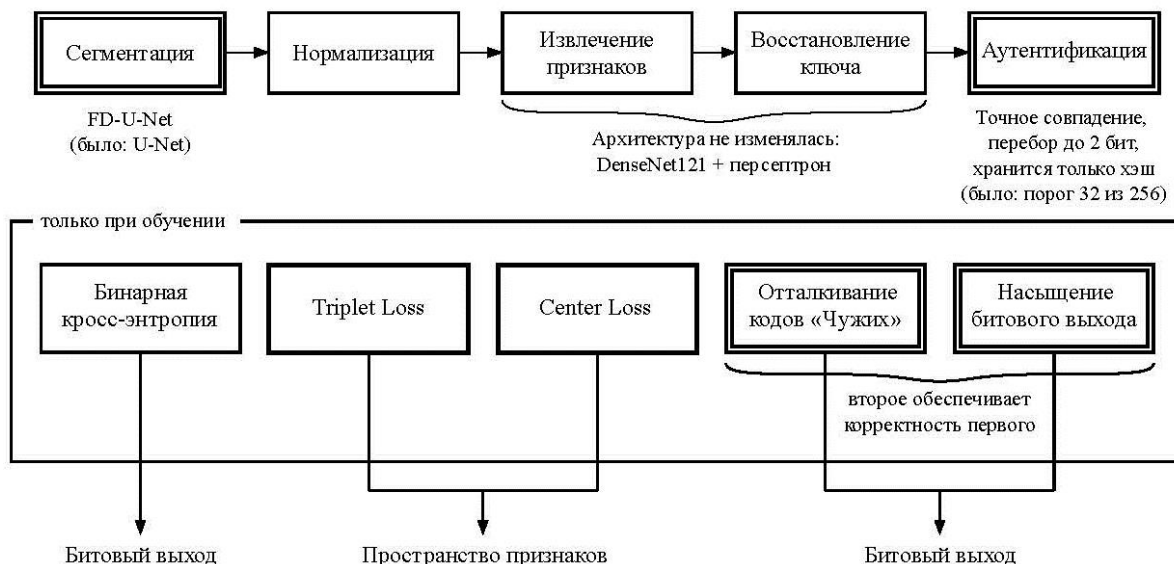


Рис. 1. Схема предлагаемого алгоритма. Двойной рамкой выделены этапы, изменённые по сравнению с решением, принятым за основу [21]; в нижней части приведены слагаемые функции потерь, используемые только при обучении

За основу принято решение [21]; изменения затрагивают выбор архитектуры сегментации, состав функции потерь при обучении и правило принятия решения при проверке, тогда как архитектура извлечения признаков и восстановления ключа оставлена без изменений. Слагаемые функции потерь, показанные в нижней части рисунка, используются только при обучении и в процедуре аутентификации не участвуют.

Выборка разделена по субъектам на пять непере-секающихся групп. Первые 50 субъектов отведены под обучение модели сегментации и исключены из последующих этапов. Ещё 50 субъектов зарегистрированы в качестве легитимных пользователей – «Своих». Оставшиеся субъекты отнесены к «Чужим» и разделены на три группы: 250 субъектов используются как отрицательные примеры при обучении, 250 субъектов образуют группу подбора порога, по которой выбирается порог бинаризации и отбирается состояние модели, а 400 субъектов составляют тестовую выборку, по которой подтверждается допуск экземпляра к эксплуатации и вычисляются приводимые далее показатели. Тестовая выборка не участвует ни в обучении, ни в отборе. Состав групп приведён в табл. 3.

Изображения «Своих» разделялись на обучающую и тестовую части в отношении 8 к 2 для каждого пользователя, что обеспечивает одинаковое число отложенных снимков у всех зарегистрированных пользователей; пересечение между частями отсутствует. Изображения «Чужих» по снимкам не разделялись – каждый глаз целиком относился к одной из трёх групп. Аугментация данных применялась только при обучении модели сегментации.

Для сегментации были исследованы четыре архитектуры: U-Net с энкодером ResNet18, IRU-Net, FD-U-Net и Lightweight U-Net. Использовались не точные копии моделей из рассмотренных исследований, а решения, построенные на лежащих в их основе идеях с унифицированными числом базовых фильтров и глубиной.

Такая унификация необходима для сопоставимости: приводимые в первоисточниках значения F1-меры получены на других наборах данных и с другой разметкой, поэтому прямое сравнение с ними некорректно, тогда как задачей табл. 4 является сравнение архитектурных решений между собой при одинаковых условиях обучения.

Таблица 3

Разбиение выборки

Группа	Субъектов	Классов	Изображений
Обучение сегментации	50	100	1 000
«Свои»	50	100	1 000
«Чужие», обучение	250	500	5 000
«Чужие», подбор порога	250	500	5 000
«Чужие», тестирование	400	800	8 000
Итого	1 000	2 000	20 000

Все модели обучались на изображениях размером 640 на 480 пикселей.

Сравнительный анализ (см. табл. 4) показал, что наилучшие значения F1-меры и коэффициента Жаккара получены у модели FD-U-Net ($F1 = 0,9712$, $IoU = 0,9442$). Различие с моделью U-Net (ResNet18) не превышает 0,0001 и лежит в пределах воспроизводимости обучения, поэтому при выборе архитектуры учитывалось также число параметров: FD-U-Net достигает того же качества при 10,1 млн параметров против 14,3 млн у U-Net (ResNet18). Данная модель использована в итоговом алгоритме.

После выделения области радужной оболочки выполнялась нормализация: использовался метод кадрирования, который, как показано в [21], обеспечивает более высокое качество последующей аутентификации по сравнению с классической нормализацией по методу Даугмана. Кадрирование представляет собой обрезку радужной оболочки по её границам (границам маски сегментации) и приведение полученного изображения к фиксированному размеру, которое в рамках данной работы составляет 256 на 256 пикселей.

Далее нормализованное изображение поступает на этап извлечения признаков и восстановления ключа. Извлечение признаков производилось предобученной свёрточной сетью DenseNet121, восстановление криптографического ключа – многослойным перцептроном (MLP). Данные модели были выбраны, так как удовлетворяют требованиям стандартов ГОСТ Р 52633.0-2006 и ГОСТ Р 52633.5-2011. Модели были объединены для совместного обучения.

Полная архитектура представлена в табл. 5.

Функция потерь строится последовательно: базовую составляющую, отвечающую за восстановление ключа, образует бинарная кросс-энтропия; к ней добавляются метрические слагаемые, формирующие признаковое пространство, и два слагаемых, действующих непосредственно в битовом выходе модели.

Для формирования максимально строгого пространства признаков, необходимого для качественного восстановления ключа, использовалась комбинированная функция потерь, включающая Triplet Loss и Center Loss.

Triplet Loss направлена на построение пространства, в котором расстояние между объектами одного класса меньше, чем между объектами разных классов, на заданную величину отступа α (margin).

Обучение происходит на тройках изображений: опорное изображение, пример того же класса и пример другого класса.

Таблица 4

Результаты сегментации с помощью различных моделей

Модель	Количество параметров	Accuracy	Precision	Recall	F1-мера	IoU
U-Net (ResNet18)	14 321 937	0,9969	0,9699	0,9726	0,9711	0,9441
FD-U-Net	10 126 241	0,9969	0,9706	0,9719	0,9712	0,9442
IRU-Net	2 772 385	0,9963	0,9611	0,9716	0,9661	0,9347
Lightweight U-Net	147 873	0,9947	0,9426	0,9606	0,9505	0,9072

Таблица 5

Архитектура модели для восстановления ключа

Модуль	Тип слоя / Операция	Входная размерность	Выходная размерность
Feature Extractor	DenseNet121	$(3, H, W)$	$(1\,024, h, w)$
Pooling	AdaptiveAvgPool2d	$(1\,024, h, w)$	$(1\,024, 1, 1)$
Flatten	Flatten	$(1\,024, 1, 1)$	1 024
Head Layer 1	Linear + BatchNorm + LeakyReLU + Dropout	1 024	768
Head Layer 2	Linear + BatchNorm + LeakyReLU + Dropout	768	512
Output Layer	Linear	512	512

Минимизация данной функции заставляет модель приближать векторы одного пользователя и отдалять векторы чужих пользователей, работая непосредственно с евклидовыми расстояниями [34]:

$$L_{\text{triplet}} = \frac{1}{|A|} \sum_{a \in A} \max(0, \|\mathbf{v}_a - \mathbf{v}_{p(a)}\|_2 - \|\mathbf{v}_a - \mathbf{v}_{n(a)}\|_2 + \alpha), \quad (9)$$

где $\mathbf{v}_a$ – вектор признаков опорного изображения, $\mathbf{v}_{p(a)}$ – вектор признаков положительного примера того же класса, $\mathbf{v}_{n(a)}$ – вектор признаков негативного примера, выбираемого из объединения признаков остальных «Своих» в мини-батче и признаков «Чужих», A – множество валидных якорей, α – параметр отступа, $\|\cdot\|_2$ – евклидова норма.

Параллельно применяется функция потерь Center Loss [35], которая штрафует модель за удаление признаков конкретного образца от центра его класса, минимизируя внутриклассовую вариацию:

$$L_{\text{center}} = \frac{1}{2B} \sum_{i=1}^B \|\mathbf{v}_i - \mathbf{c}_{y_i}\|_2^2, \quad (10)$$

где B – количество примеров в текущем мини-батче, $\mathbf{v}_i$ – вектор признаков i -го примера в батче, y_i – метка класса (пользователя) для i -го примера, $\mathbf{c}_{y_i}$ – текущий вектор-центр класса y_i .

Метрические слагаемые действуют в пространстве признаков и не гарантируют, что сам битовый выход не окажется близок к одному из ключей базы: при насыщении функций потерь Triplet Loss и Center Loss восстановленный код «Чужого» может подойти к базе вплотную. Поэтому введены два слагаемых – L_{rep} (отталкивание, repulsion) и L_{bin} (бинаризация, binarization), работающих непосредственно в битовом выходе.

Первое отталкивает коды «Чужих» от базы ключей. Для каждого «Чужого» из обучающей выборки вычисляется мягкое расстояние Хэмминга от вероятностей на выходе модели до каждого ключа базы, берётся минимальное, и, если оно меньше заданного запаса, начисляется штраф, пропорциональный недостающей величине. В отличие от метрических слагаемых, оно действует в той же величине, в которой измеряется минимальное расстояние Хэмминга, поэтому позволяет удерживать его на заданном уровне.

Второе насыщает битовый выход: штрафуются величина $p(1-p)$, где p – вероятность на выходе модели; она максимальна при $p = 0,5$ и обращается в нуль при значениях, близких к нулю и единице. Это

слагаемое необходимо для корректности первого: при ненасыщенных выходах мягкое расстояние Хэмминга расходится с фактическим расстоянием после бинаризации, и код «Чужого» может совпасть с ключом базы, тогда как мягкое расстояние остаётся большим и отталкивание не срабатывает. Дополнительно насыщение делает устойчивее выбор порога бинаризации. Оба слагаемых используются только при обучении: при аутентификации они не применяются и никаких вспомогательных данных не сохраняется.

Общая функция потерь L_{key} для совместного обучения модели корректному восстановлению ключа и формирования детерминированного признакового пространства формируется как взвешенная сумма компонент:

$$L_{\text{key}} = L_{\text{BCEWithLogitsLoss}} + \lambda_t \cdot L_{\text{triplet}} + \lambda_c \cdot L_{\text{center}} + \lambda_{\text{rep}} \cdot L_{\text{rep}} + \lambda_{\text{bin}} \cdot L_{\text{bin}}, \quad (11)$$

где $L_{\text{BCEWithLogitsLoss}}$ – бинарная кросс-энтропия с логитами, объединяющая в себе сигмоидное преобразование и вычисление бинарной кросс-энтропии в одной численно устойчивой операции. Данная функция потерь напрямую минимизирует ошибку восстановления ключа; $\lambda_t, \lambda_c, \lambda_{\text{rep}}, \lambda_{\text{bin}} > 0$ – гиперпараметры, регулирующие вклад остальных компонент.

Значения весовых коэффициентов определялись с учётом масштаба соответствующих слагаемых. Поскольку векторы признаков нормируются, значения функций потерь Triplet Loss и Center Loss лежат в сопоставимых пределах, что допускает использование коэффициентов одного порядка; их итоговые значения ($\lambda_t = 1,0$, $\lambda_c = 0,5$, $\lambda_{\text{rep}} = 0,3$, $\lambda_{\text{bin}} = 0,1$) подбирались вручную по нескольким пробным обучением; отдельного автоматического поиска не проводилось.

Анализ эффективности предлагаемого алгоритма

Отбор состояния модели и допуск экземпляра к эксплуатации разнесены по разным группам «Чужих». В ходе обучения сохраняется то состояние, у которого на группе подбора порога отсутствуют ложные допуски, а минимальное расстояние Хэмминга между восстановленными кодами «Чужих» и базой ключей составляет не менее 18 бит. Отобранное состояние допускается к эксплуатации, если на тестовой выборке ложные допуски также отсутствуют, а минимальное расстояние составляет не менее пяти бит; экземпляр, не удовлетворяющий этому условию, отбраковывается, и обучение повторяется с другой инициализацией. Величина запаса задана до серии

обучений как кратно превышающая требуемые пять бит. Достаточность выбранного значения проверена отдельным расчётом без переобучения, в котором при фиксированном состоянии модели порог подбирался заново для разных значений запаса: у обоих допущенных экземпляров требование пяти бит на тестовой выборке выполняется, начиная с запаса 18 бит, тогда как при 16 битах минимальное расстояние у одного из них падает до трёх. Расчёт носит апостериорный характер и на отбор состояний не влиял. Среди допустимых конфигураций предпочтение отдаётся той, у которой доля истинного принятия максимальна, а при различии в пределах разброса между независимыми обучениями – более воспроизводимой.

Переход к комбинированной функции потерь, включающей Triplet Loss и Center Loss, позволил получить состояния, удовлетворяющие введённому критерию. В качестве рабочей принята конфигурация с восемью обучаемыми блоками свёрточной сети; из трёх независимых обучений допуск к эксплуатации получили два. Для допущенных экземпляров доля истинного принятия составила 0,870 и 0,880, вероятность ошибки первого рода – 0,130 и 0,120, а вероятность ошибки второго рода оказалась нулевой: ни одного ложного допуска на 8000 предъявлений «Чужих» из тестовой выборки. Минимальное расстояние Хэмминга между восстановленными кодами «Чужих» и базой ключей составило 10 и 7 бит при медиане 201 и 227 бит; ближе двадцати бит к базе ключей оказались 4 и 3 предъявления из восьми тысяч. Влияние числа обучаемых блоков свёрточной сети приведено в табл. 6.

Качество восстановления ключа монотонно возрастает с увеличением числа обучаемых блоков и выходит на насыщение начиная с восьми блоков, где доля истинного принятия составляет $0,873 \pm 0,006$ против $0,877 \pm 0,050$ при десяти и $0,895 \pm 0,074$ при двенадцати блоках. Различия между этими тремя конфигурациями лежат внутри разброса между независимыми обучениями. Доля обучений, получивших допуск к эксплуатации, при этом не возрастает и составляет два из трёх при восьми и десяти блоках и одно из трёх при двенадцати.

Из протоколов обучения видно, что с увеличением числа размороженных блоков модель точнее подгоняет коды зарегистрированных пользователей

под назначенные им ключи, тогда как расстояние от восстановленных кодов «Чужих» до базы ключей при этом не возрастает. Условию отбора на группе подбора порога удовлетворяет подавляющее большинство эпох; количественно это показано далее. Следовательно, различие между конфигурациями проявляется не в доступности допустимых состояний, а в том, сохраняется ли достигнутый при отборе запас на тестовой выборке.

Выбор восьми блоков обоснован тем, что при статистически неразличимых значениях доли истинного принятия алгоритм даёт наименьший разброс между независимыми обучениями: 0,006 против 0,050 при десяти блоках и 0,074 при двенадцати. Тот же порядок сохраняется и для разброса вероятности ошибки первого рода при переборе в окрестности радиуса два бита: 0,003 против 0,044 при десяти блоках и 0,053 при двенадцати. Порог бинаризации при восьми блоках изменяется в более широких пределах: от 0,82 до 0,92, тогда как при десяти блоках он принимает значения от 0,84 до 0,86; на итоговые показатели это не влияет, поскольку порог подбирается для каждого обученного экземпляра отдельно и между обучениями не переносится.

Подтверждение допуска на тестовой выборке оказалось заметно более строгим, чем отбор на группе подбора порога. Условию отбора с запасом 18 бит удовлетворяло от 76 до 98% эпох в каждом обучении (при восьми и более обучаемых блоках – от 95 до 98%), тогда как требование пяти бит на тестовой выборке сохранилось в девяти обучениях из двадцати одного. Нарушение вызывается небольшим числом отдельных предъявлений: в обучении, не получивших допуска, условию не удовлетворяли от одного до шести снимков, принадлежавших одному-четырёх субъектам, при том, что медиана расстояний до базы ключей оставалась в пределах от 200 до 220 бит. Таким образом, распределение расстояний в целом не ухудшается, нарушается его левый край.

Увеличение запаса при подборе порога положения не исправляет. У экземпляров, получивших допуск, требование пяти бит выполняется начиная с запаса 10 и 18 бит, а с дальнейшим ростом запаса минимальное расстояние на тестовой выборке монотонно увеличивается и при запасе 40 бит достигает 32 и 18 бит.

Таблица 6

Влияние числа обучаемых блоков свёрточной нейронной сети (100 «Своих», по три независимых обучения на конфигурацию)*

Обучаемых блоков	Доля истинного принятия	Вероятность ошибки первого рода	Обучений, получивших допуск	Минимальное расстояние Хэмминга по обучением, бит
0	$0,062 \pm 0,010$	$0,938 \pm 0,010$	2 из 3	2, 11, 6
2	$0,275 \pm 0,048$	$0,725 \pm 0,048$	0 из 3	0, 0, 1
4	$0,627 \pm 0,066$	$0,373 \pm 0,066$	1 из 3	1, 13, 0
6	$0,775 \pm 0,041$	$0,225 \pm 0,041$	1 из 3	1, 0, 13
8	$0,873 \pm 0,006$	$0,127 \pm 0,006$	2 из 3	10, 0, 7
10	$0,877 \pm 0,050$	$0,123 \pm 0,050$	2 из 3	10, 0, 7
12	$0,895 \pm 0,074$	$0,105 \pm 0,074$	1 из 3	2, 22, 0

*Отбор на группе подбора порога прошли все обучения; в четвёртом столбце указано, в скольких из них требование минимального расстояния сохранилось на тестовой выборке. У допущенных экземпляров ложных допусков не зафиксировано.

У экземпляра, не получившего допуска, оно остаётся нулевым при любом запасе в диапазоне от 4 до 40 бит: код одного из «Чужих» совпадает с ключом базы при всех значениях порога бинаризации, и выбором порога это совпадение не устраняется. Следовательно, запас улучшает калибровку исправного экземпляра, но не заменяет проверку на отдельной группе, а объём самой группы влияет на результат самостоятельно: минимум по выборке не возрастает с ростом её объёма, поэтому оценка по 5000 предъявлений не может быть строже оценки по 8000. Определение необходимого объёма группы, в том числе за счёт синтетического порождения изображений «Чужих», составляет предмет дальнейшей работы.

Снижение вероятности ложного отказа за счёт перебора в окрестности Хэмминга

Несмотря на нулевую оценку вероятности ложного допуска, в рассматриваемой системе сохраняется проблема ложных отказов, обусловленная требованием точного побитового совпадения восстановленного криптографического ключа с эталонным. Даже при высокой разделимости признаков пространства отдельные биты ключей восстанавливаются с ошибками, что приводит к отклонению легитимного пользователя при строгом критерии полного совпадения.

С учётом того, что ошибки восстановления ключа для одного и того же пользователя, как правило, носят локальный характер и затрагивают ограниченное число позиций, был рассмотрен подход, основанный на проверке принадлежности восстановленного ключа окрестности в пространстве Хэмминга. В рамках данного подхода при аутентификации анализируется не только исходный предсказанный ключ, но и множество ключей, находящихся на расстоянии не более k по метрике Хэмминга. Таким образом, задача проверки сводится к поиску совпадения в ограниченной области вокруг восстановленного вектора бинарного кода.

Размер этой области определяется параметром k . При $k = 1$ выполняется проверка всех вариантов, отличающихся ровно в одном бите, что соответствует 512 дополнительным кандидатам для ключа длиной 512 бит. При $k = 2$ число рассматриваемых комбинаций возрастает до $1,3 \cdot 10^5$, что существенно увеличивает вычислительную нагрузку, но остаётся допустимым при ограниченном числе попыток аутентификации.

Выбор допустимого радиуса поиска определяется структурой межклассовых расстояний в пространстве ключей. В проведённых экспериментах минимальное расстояние между восстановленными кодами «Чужих» и базой ключей у допущенных к эксплуатации экземпляров составило 7 и 10 бит. В этих условиях увеличение радиуса до $k = 1$ и $k = 2$ позволяет компенсировать наиболее вероятные ошибки восстановления, не приводя к заметному ухудшению разделимости ключей. Наименьшее из наблюдавшихся значений формально допускает радиус до шести бит, однако число проверяемых кандидатов

растёт комбинаторно и при трёх битах превышает $2,2 \cdot 10^7$, поэтому радиус ограничен двумя битами.

Перебор в окрестности Хэмминга прямо предусмотрен ГОСТ Р 52633.0–2006 [3]: п. 5.7 допускает оснащение средства высокондёжной биометрической аутентификации системой перебора возможных состояний наиболее нестабильных бит выходного ключа и разрешает перебор в пределах 7% бит ключа. Используемый в работе радиус два бита при длине ключа 512 бит соответствует 0,39% бит, т.е. лежит внутри допустимого предела с большим запасом. При этом предлагаемая схема не формирует и не хранит сведений о положении нестабильных разрядов: перебор ведётся по всей окрестности, поэтому требование стандарта об уничтожении такой информации к ней не относится. В традиционных системах подобные задачи решаются либо введением порога на расстояние Хэмминга, либо применением кодов коррекции ошибок и схем нечёткой экстракции признаков [21, 29]. В отличие от этих методов, в данной работе корректировка ошибок выполняется на этапе проверки путём локального поиска в пространстве бинарных ключей без ослабления требования полного совпадения ключа, что допускает хэширование, и без использования дополнительной вспомогательной информации.

Экспериментальные результаты показывают, что применение данного подхода позволяет снизить вероятность ложного отказа. Для рабочей конфигурации при разрешении одной битовой ошибки среднее значение вероятности ошибки первого рода уменьшается с 0,125 до 0,115, а при увеличении радиуса поиска до двух бит – до 0,107. Ложных допусков при этом не появляется: радиус поиска остаётся строго меньше минимального расстояния от восстановленных кодов «Чужих» до базы ключей, составляющего у допущенных экземпляров 7 и 10 бит.

Распределение расстояний Хэмминга между восстановленными кодами «Своих» и базой ключей носит двухмодальный характер: подавляющая часть снимков даёт точное совпадение либо отличается на один-два бита, тогда как оставшиеся отклонения составляют десятки и сотни бит. Соответственно, перебор в окрестности Хэмминга устраняет примерно седьмую часть отказов (те из них, которые вызваны единичными и парными искажениями битов), но не влияет на отказы второй группы, которые не могут быть компенсированы никаким практически выполнимым перебором. Дальнейшее снижение вероятности ложного отказа связано не с увеличением радиуса поиска, а с контролем качества предъявляемого изображения.

Дополнительно рассмотрен режим, допускающий вторую попытку аутентификации. ГОСТ Р 52633.0–2006 [3] (п. 5.6) допускает предоставление пользователю нескольких попыток аутентификации и указывает, что их число может быть сопоставимо с числом примеров образа «Свой», на которых обучалась система. Предположение о независимости попыток, однако, для биометрической аутентификации не

выполняется: отказы одного и того же пользователя порождаются устойчивыми свойствами его изображений, а не независимым шумом. Поэтому вероятность отказа при двух попытках не вычислялась как произведение вероятностей, а измерялась непосредственно.

Для измерения использовалось разбиение, при котором у каждого зарегистрированного пользователя отложены ровно два снимка, не участвовавших в обучении; таким образом, каждая пара отложенных снимков представляет собой реализацию режима двух попыток. Для рабочей конфигурации отказ по обоим попыткам наблюдался у 1 пользователя из 100 при требовании точного совпадения ключа в каждом из двух допущенных обучений; при переборе в окрестности радиуса два бита он сохранился лишь в одном из них. Единичное событие не позволяет судить о зависимости попыток по отдельному обучению, поэтому она оценивалась по совокупности обучений в области насыщения. На 900 парах, полученных в девяти обучении при восьми, десяти и двенадцати блоках, двойной отказ наблюдался 25 раз при 13,8, ожидаемых в предположении независимости. Значимость проверена точным перестановочным критерием: в каждом обучении число отказавших снимков фиксировалось, отказы случайным образом распределялись по снимкам, и доля перестановок, дающих 25 и более двойных отказов, оказалась меньше 0,001. Условная вероятность отказа второй попытки при отказе первой составила 0,235 против безусловной 0,118 по этим же девяти обучением. Следовательно, оценка по произведению вероятностей занижает вероятность двойного отказа примерно в 1,8 раза и в качестве расчётной приниматься не может.

Влияние повторной попытки на вероятность ложного допуска оценивалось сверху. По неравенству Буля вероятность ложного допуска хотя бы в одной из k попыток не превышает произведения k на вероятность ложного допуска при одной попытке; данная оценка справедлива при любой зависимости между попытками и не требует дополнительных предположений. У допущенных к эксплуатации экземпляров ложных допусков на тестовой выборке не зафиксировано, и вторая попытка этого вывода не меняет: она удваивает число предъявлений, но не сокращает расстояние от восстановленных кодов «Чужих» до базы ключей, минимум которого составляет 7 и 10 бит при радиусе поиска два бита.

Заключение

В ходе выполнения работы модифицирован и экспериментально исследован нейросетевой алгоритм высоконадёжной биометрической аутентификации по радужной оболочке глаза. Основные результаты работы могут быть резюмированы в следующих положениях:

1. Проведён анализ современных методов сегментации, извлечения признаков и аутентификации по радужной оболочке глаза. Установлено, что нейросетевые подходы обеспечивают существенно более высокую точность выделения радужной обо-

лочку по сравнению с граничными методами, а метрические функции потерь позволяют формировать признаковое пространство, пригодное для последующего восстановления криптографического ключа. Обосновано также, что сиамские архитектуры и сквозные преобразователи, успешные в задачах идентификации, для высоконадёжной аутентификации неприменимы по требованиям ГОСТ Р 52633.

2. Предложен и реализован алгоритм, включающий сегментацию с помощью сети FD-U-Net, нормализацию кадрированием, извлечение признаков сетью DenseNet121 и восстановление криптографического ключа многослойным персептроном. Выбор FD-U-Net обоснован наилучшим значением F1-меры (0,9712) среди исследованных архитектур при числе параметров меньшем, чем у ближайшей по качеству модели.

3. Экспериментально подтверждена эффективность комбинированной функции потерь, включающей Triplet Loss и Center Loss, в сочетании с двумя дополнительными членами, действующими в битовом выходе модели. Для экземпляров, допущенных к эксплуатации, аутентификация по точному побитовому совпадению 512-битного криптографического ключа обеспечена при нулевой вероятности ложного допуска (ни одного ложного допуска на 8000 предъявлений «Чужих» из тестовой выборки, минимальное расстояние до базы ключей 10 и 7 бит) и вероятности ошибки первого рода 0,130 и 0,120, снижаемой до 0,110 и 0,105 перебором в окрестности радиуса два бита. Измеренная вероятность отказа при двух попытках составила 0,010 при требовании точного совпадения ключа и 0,005 при переборе в окрестности радиуса два бита. Судить о зависимости попыток по одному обучению это число не позволяет; по совокупности обучений двойной отказ происходит примерно в 1,8 раза чаще, чем предсказывает предположение о независимости, поэтому расчёт по произведению вероятностей для данной задачи неприменим. Установлено также, что запас, обеспечиваемый на группе подбора порога из 250 субъектов, переносится на тестовую выборку из 400 субъектов лишь частично, что определяет объём этой группы как самостоятельный параметр системы; влияние объёма группы «Чужих», используемой при обучении, предстоит оценить отдельно.

Практическая значимость работы заключается в том, что предложенный алгоритм позволяет отказаться от хранения криптографических ключей и биометрических эталонов в открытом виде: проверка выполняется по хэшу точно восстановленного ключа. Ключ формируется криптографическим генератором случайных чисел, не выводится из биометрических данных и имеет длину 512 бит при требовании энтропии не менее 128 бит; преобразователь «биометрия-код» реализован многослойным персептроном, допускающим послойное обучение.

Предложенные решения могут быть использованы при разработке систем аутентификации для критически важных информационных ресурсов.

Литература

1. Information security methods – modern research directions / A. Shelupanov, O. Evsyutin, A. Konev, E. Kostyuchenko, D. Kruchinin, D. Nikiforov // *Symmetry*. – 2019. – Vol. 11, No. 2. – P. 150.
2. Nguyen K. Deep learning for iris recognition: a survey / K. Nguyen, H. Proença, F. Alonso-Fernandez // *ACM Computing Surveys*. – 2024. – Vol. 56, No. 9. – P. 1–35.
3. ГОСТ Р 52633.0–2006. Защита информации. Техника защиты информации. Требования к средствам высоконадежной биометрической аутентификации. – М.: Стандартинформ, 2020. – 19 с.
4. Müller D. Towards a guideline for evaluation metrics in medical image segmentation / D. Müller, I. Soto-Rey, F. Kramer // *BMC Research Notes*. – 2022. – Vol. 15, No. 1. – P. 210.
5. Mayya A. Iris and palmprint decision fusion to enhance human recognition / A. Mayya, M. Saii // *International Journal of Computer Science Trends and Technology*. – 2017. – Vol. 5. – P. 42–46.
6. Семёнов М.С. Сравнение методов сегментации изображения радужной оболочки глаза / М.С. Семёнов, Е.В. Мясников // *Информационные технологии и нанотехнологии (ИТНТ-2018): сб. трудов IV Междунар. конф. и молодёжной школы, Самара, 24–27 апреля 2018 г.* – Самара: Самар. нац. исслед. ун-т им. акад. С.П. Королева, 2018. – С. 814–821.
7. Daugman J.G. High confidence visual recognition of persons by a test of statistical independence // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. – 1993. – Vol. 15, No. 11. – P. 1148–1161.
8. Чигринский В.В. Быстрый алгоритм поиска границ зрачка и радужной оболочки глаза / В.В. Чигринский, Ю.С. Ефимов, И.А. Матвеев // *Машинное обучение и анализ данных*. – 2016. – Т. 2, № 2. – С. 159–172.
9. Ганеева Ю.Х. Сегментация радужной оболочки глаза на изображении с помощью свёрточной нейронной сети архитектуры U-Net / Ю.Х. Ганеева, Е.В. Мясников // *Информационные технологии и нанотехнологии (ИТНТ-2020): сб. трудов VI Междунар. конф. и молодёжной школы, Самара, 26–29 мая 2020 г.* – Самара: Самар. нац. исслед. ун-т им. акад. С.П. Королева, 2020. – Т. 2. – С. 57–63.
10. Ronneberger O. U-Net: convolutional networks for biomedical image segmentation / O. Ronneberger, P. Fischer, T. Brox // *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015: proc. of the 18th Int. Conf., Munich, Germany, October 5–9, 2015*. – Cham: Springer, 2015. – P. 234–241.
11. Lozej J. End-to-end iris segmentation using U-Net / J. Lozej, B. Meden, V. Struc, P. Peer // *2018 IEEE International Work Conference on Bioinspired Intelligence (IWOBI)*, July 18–20, 2018. – San Carlos, Costa Rica: IEEE, 2018. – P. 1–6. DOI: 10.1109/IWOBI.2018.8464213.
12. A robust iris segmentation scheme based on improved U-Net / W. Zhang, X. Lu, Y. Gu, Y. Liu, X. Meng, J. Li // *IEEE Access*. – 2019. – Vol. 7. – P. 85082–85089.
13. Wu X. Study on iris segmentation algorithm based on dense U-Net / X. Wu, L. Zhao // *IEEE Access*. – 2019. – Vol. 7. – P. 123959–123968.
14. Robust iris segmentation algorithm in non-cooperative environments using interleaved residual U-Net / Y.H. Li, W.R. Putri, M.S. Aslam, C.C. Chang // *Sensors*. – 2021. – Vol. 21, No. 4. – P. 1434.
15. Efficient and robust eye images iris segmentation using a lightweight U-Net convolutional network / C. Miron, A. Pasarica, V. Manta, R. Timofte // *Multimedia Tools and Applications*. – 2022. – Vol. 81, No. 11. – P. 14961–14977.
16. Farmanifard P. Iris-SAM: iris segmentation using a foundation model / P. Farmanifard, A. Ross // *Pattern Recognition and Artificial Intelligence: proc. of the 4th Int. Conf. ICPRAI 2024, Jeju Island, South Korea, July 3–6, 2024*. – Singapore: Springer Nature Singapore, 2024. – P. 394–409.
17. Uncertainty-aware bilateral transformer for accurate and reliable iris segmentation / J. Wei, X. Gao, Y. Wang, R. He, Z. Sun // *IEEE Transactions on Information Forensics and Security*. – 2025. – Vol. 20. – P. 5919–5933.
18. Jiang J. SAM-Iris: a SAM-based iris segmentation algorithm / J. Jiang, Q. Zhang, C. Wang // *Electronics*. – 2025. – Vol. 14, No. 2. – P. 246.
19. IrisST-Net for iris segmentation and contour parameters extraction / Y. Liu, W. Shen, D. Wu, J. Shao // *Applied Intelligence*. – 2023. – Vol. 53, No. 9. – P. 11267–11281.
20. Ganeeva Y.K. Identifying persons from iris images using neural networks for image segmentation and feature extraction / Y.K. Ganeeva, E.V. Myasnikov // *Computer Optics*. – 2022. – Vol. 46, No. 2. – P. 308–316.
21. Штука С.Е. Разработка нейросетевого алгоритма высоконадежной биометрической аутентификации на основе радужной оболочки глаза / С.Е. Штука, А.Е. Боршевников // *Региональная информатика и информационная безопасность: сб. трудов XIV Санкт-Петербургской межрегион. конф., Санкт-Петербург, 29–31 октября 2025 г.* – СПб.: СПОИСУ, 2025. – С. 204–206.
22. Demirel H. Iris recognition system using combined histogram statistics / H. Demirel, G. Anbarjafari // *2008 23rd International Symposium on Computer and Information Sciences (ISCIS)*, October 27–29, 2008. – Istanbul, Turkey: IEEE, 2008. – P. 1–4.
23. Monro D.M. DCT-based iris recognition / D.M. Monro, S. Rakshit, D. Zhang // *IEEE Transactions on Pattern Analysis and Machine Intelligence*. – 2007. – Vol. 29, No. 4. – P. 586–595.
24. An effective model for the iris regional characteristics and classification using deep learning Alex network / T. Balashanmugam, K. Sengottaiyan, M.S. Kulandairaj, H. Dang // *IET Image Processing*. – 2023. – Vol. 17, No. 1. – P. 227–238.
25. Iris recognition based on local circular Gabor filters and multi-scale convolution feature fusion network / J. Sun, S. Zhao, Y. Yu, X. Wang, L. Zhou // *Multimedia Tools and Applications*. – 2022. – Vol. 81, No. 23. – P. 33051–33065.
26. Li Y. A survey on Siamese network: methodologies, applications, and opportunities / Y. Li, C.L.P. Chen, T. Zhang // *IEEE Transactions on Artificial Intelligence*. – 2022. – Vol. 3, No. 6. – P. 994–1014.
27. Latif S.A. Hybrid CNN-ViT integration into Siamese networks for robust iris biometric verification / S.A. Latif, K.A. Sidek, A.H.A. Hashim // *Bulletin of Electrical Engineering and Informatics*. – 2025. – Vol. 14, No. 4. – P. 3101–3109.
28. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия–код доступа. – М.: Стандартинформ, 2018. – 16 с.
29. Quantifying privacy and security of biometric fuzzy commitment / X. Zhou, A. Kuijper, R. Veldhuis, C. Busch // *2011 International Joint Conference on Biometrics (IJCB)*, Washington, DC, USA, October 11–13, 2011. – IEEE, 2011. – P. 1–8.
30. Kausar F. Iris based cancelable biometric cryptosystem for secure healthcare smart card // *Egyptian Informatics Journal*. – 2021. – Vol. 22, No. 4. – P. 447–453.
31. Matveev I. From iris image to embedded code: system of methods / I. Matveev, I. Safonov // *Algorithms*. – 2023. – Vol. 16, No. 2. – Art. 87.

32. Lin K.-C. A high-security-level iris cryptosystem based on fuzzy commitment and soft reliability extraction / K.-C. Lin, Y.-M. Chen // IEEE Transactions on Dependable and Secure Computing. – 2024. – Vol. 21, No. 4. – P. 1770–1784.

33. Fuzzy extractors are practical: cryptographic strength key derivation from the iris / A. Shukla, L. Demarest, B. Fuller, S. Ahmad, C. Manicke, A. Russell, S. Chen // Proceedings of the 2025 ACM SIGSAC Conference on Computer and Communications Security (CCS '25), Taipei, Taiwan, October 13–17, 2025. – New York: ACM, 2025. – P. 3605–3619.

34. Schroff F. FaceNet: a unified embedding for face recognition and clustering / F. Schroff, D. Kalenichenko, J. Philbin // 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), June 7–12, 2015. – Boston, MA, USA: IEEE, 2015. – P. 815–823.

35. A discriminative feature learning approach for deep face recognition / Y. Wen, K. Zhang, Z. Li, Y. Qiao // Computer Vision – ECCV 2016: proc. of the 14th European Conf., Amsterdam, The Netherlands, October 11–14, 2016. – Cham: Springer, 2016. – P. 499–515.

Штука Станислав Евгеньевич

Студент департамента информационной безопасности
Дальневосточного федерального университета (ДВФУ)
п. Аякс, о. Русский, 10, г. Владивосток, Россия, 690922
ORCID: 0009-0007-0659-6166
Тел.: +7-914-712-25-67
Эл. почта: stanislav.shtuka@mail.ru

Боршевников Алексей Евгеньевич

Ст. аналитик АО «Промышленные криптосистемы»
(АО «ПроКСи»)
Отрадная ул., 2Б, стр. 1, г. Москва, Россия, 127273
ORCID: 0000-0002-7383-1820
Тел.: +7-924-131-67-97
Эл. почта: borshevnikov.ae@dvfu.ru

Поступила в редакцию: 29.05.2026.

Принята к публикации: 12.08.2026.

Shtuka S.E., Borshevnikov A.E.

Modification of a neural network algorithm for highly reliable iris-based biometric authentication

Relevance. The growing number of systems processing confidential data calls for authentication mechanisms that remain secure when the stored reference data is compromised. **Purpose of the study.** To modify a neural network algorithm for highly reliable iris-based biometric authentication, enabling the cryptographic key recovery with an exact bit-wise match. **Methods.** A convolutional neural network is used to extract the iris region, followed by crop-based normalization. Joint training of a convolutional model for feature extraction and a multi-layer perceptron is performed using a combined loss function comprising metric terms and two terms acting directly on the bit-wise output of the model. The operating point is selected according to an admissibility criterion, and Hamming-neighborhood search is employed at the verification stage. **Scientific novelty.** Unlike known schemes, exact key recovery is achieved without auxiliary data or external error correction, allowing only the hash of the key to be stored. **Results.** For 100 enrolled users, the genuine acceptance rate among the instances admit-

ted for operation was 0.875 with a zero false acceptance probability over 8000 impostor presentations. Searching within a radius of two bits reduces the type I error probability to 0.107 without changing the type II error probability. Rejection on both attempts under exact key match was observed for 1 out of 100 users. It is shown that the margin secured on the threshold-selection group transfers to the test set only in part. **Practical significance.** The algorithm is applicable in systems where the storage of biometric reference data and cryptographic keys in plaintext is unacceptable.

Keywords: biometric authentication, iris recognition, image segmentation, neural networks, cryptographic key, Triplet Loss, Center Loss, biometric cryptography.

DOI: 10.21293/1818-0442-2026-29-2-148-159

References

1. Shelupanov A., Evsyutin O., Konev A., Kostyuchenko E., Kruchinin D., Nikiforov D. Information security methods – modern research directions. *Symmetry*, 2019, vol. 11, no. 2, art. 150.
2. Nguyen K., Proença H., Alonso-Fernandez F. Deep learning for iris recognition: a survey. *ACM Computing Surveys*, 2024, vol. 56, no. 9, pp. 1–35.
3. GOST R 52633.0-2006. *Zashchita informatsii. Tekhnika zashchity informatsii. Trebovaniya k sredstvam vysokonadezhnoy biometricheskoj autentifikatsii* [Information protection. Information protection technique. Requirements for means of high-reliability biometric authentication]. Moscow, Standartinform Publ., 2020 (in Russ.).
4. Müller D., Soto-Rey I., Kramer F. Towards a guideline for evaluation metrics in medical image segmentation. *BMC Research Notes*, 2022, vol. 15, no. 1, art. 210.
5. Mayya A., Saii M. Iris and palmprint decision fusion to enhance human recognition. *International Journal of Computer Science Trends and Technology*, 2017, vol. 5, no. 5, pp. 42–46.
6. Semyonov M.S., Myasnikov E.V. *Sravnenie metodov segmentatsii izobrazheniya raduzhnoy obolochki glaza* [Comparison of iris image segmentation methods]. *Informatsionnye tekhnologii i nanotekhnologii (ITNT-2018)* [Information Technologies and Nanotechnologies]. Proc. of the IV Int. Conf., Samara, 24–27 April 2018, Samara, Samara National Research University named after Academician S.P. Korolev, 2018, pp. 814–821 (in Russ.).
7. Daugman J.G. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1993, vol. 15, no. 11, pp. 1148–1161.
8. Chigrinskiy V.V., Efimov Yu.S., Matveev I.A. *Bystryy algoritm poiska granits zrachka i raduzhnoy obolochki glaza* [A fast algorithm for locating pupil and iris boundaries]. *Mashinnoe obuchenie i analiz dannykh*, 2016, vol. 2, no. 2, pp. 159–172 (in Russ.).
9. Ganeeva Yu.Kh., Myasnikov E.V. *Segmentatsiya raduzhnoy obolochki glaza na izobrazhenii s pomoshchyu svertochnoy neyronnoy seti arkhitektury U-Net* [Iris segmentation in an image using a U-Net convolutional neural network]. *Informatsionnye tekhnologii i nanotekhnologii (ITNT-2020)* [Information Technologies and Nanotechnologies]. Proc. of the VI Int. Conf., Samara, 26–29 May 2020, Samara, Samara National Research University named after Academician S.P. Korolev, 2020, vol. 2, pp. 57–63 (in Russ.).
10. Ronneberger O., Fischer P., Brox T. U-Net: convolutional networks for biomedical image segmentation. Proc. of the 18th Int. Conf.: Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015, Munich, Germany, Cham, Springer, 2015, pp. 234–241.

11. Lozej J., Meden B., Struc V., Peer P. End-to-end iris segmentation using U-Net. 2018 IEEE International Work Conference on Bioinspired Intelligence (IWOB), San Carlos, Costa Rica, IEEE, 2018, pp. 1–6. DOI: 10.1109/IWOB.2018.8464213.
12. Zhang W., Lu X., Gu Y., Liu Y., Meng X., Li J. A robust iris segmentation scheme based on improved U-Net. *IEEE Access*, 2019, vol. 7, pp. 85082–85089.
13. Wu X., Zhao L. Study on iris segmentation algorithm based on dense U-Net. *IEEE Access*, 2019, vol. 7, pp. 123959–123968.
14. Li Y.H., Putri W.R., Aslam M.S., Chang C.C. Robust iris segmentation algorithm in non-cooperative environments using interleaved residual U-Net. *Sensors*, 2021, vol. 21, no. 4, p. 1434.
15. Miron C., Pasarica A., Manta V., Timofte R. Efficient and robust eye images iris segmentation using a lightweight U-Net convolutional network. *Multimedia Tools and Applications*, 2022, vol. 81, no. 11, pp. 14961–14977.
16. Farmanifard P., Ross A. Iris-SAM: iris segmentation using a foundation model. Pattern Recognition and Artificial Intelligence. Proc. of the 4th Int. Conf. ICPRAI 2024, Jeju Island, South Korea, Singapore, Springer Nature Singapore, 2024, pp. 394–409.
17. Wei J., Gao X., Wang Y., He R., Sun Z. Uncertainty-aware bilateral transformer for accurate and reliable iris segmentation. *IEEE Transactions on Information Forensics and Security*, 2025, vol. 20, pp. 5919–5933.
18. Jiang J., Zhang Q., Wang C. SAM-Iris: a SAM-based iris segmentation algorithm. *Electronics*, 2025, vol. 14, no. 2, p. 246.
19. Liu Y., Shen W., Wu D., Shao J. IrisST-Net for iris segmentation and contour parameters extraction. *Applied Intelligence*, 2023, vol. 53, no. 9, pp. 11267–11281.
20. Ganeeva Y.K., Myasnikov E.V. Identifying persons from iris images using neural networks for image segmentation and feature extraction. *Computer Optics*, 2022, vol. 46, no. 2, pp. 308–316.
21. Shtuka S.E., Borshevnikov A.E. *Razrabotka neyrosetevogo algoritma vysokonadezhnoy biometricheskoy autentifikatsii na osnove raduzhnoy obolochki glaza* [Development of a neural network algorithm for high-reliability biometric authentication based on the iris]. *Regionalnaya informatika i informatsionnaya bezopasnost. [Regional Informatics and Information Security]* Proc. of the XIV St. Petersburg Interregional Conf., St. Petersburg, 29–31 October 2025, St. Petersburg, SPOISU Publ., 2025, pp. 204–206 (in Russ.).
22. Demirel H., Anbarjafari G. Iris recognition system using combined histogram statistics. 2008 23rd International Symposium on Computer and Information Sciences (ISCIS), Istanbul, Turkey, IEEE, 2008, pp. 1–4.
23. Monro D.M., Rakshit S., Zhang D. DCT-based iris recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 2007, vol. 29, no. 4, pp. 586–595.
24. Balashanmugam T., Sengottaiyan K., Kulandairaj M.S., Dang H. An effective model for the iris regional characteristics and classification using deep learning Alex network. *IET Image Processing*, 2023, vol. 17, no. 1, pp. 227–238.
25. Sun J., Zhao S., Yu Y., Wang X., Zhou L. Iris recognition based on local circular Gabor filters and multi-scale convolution feature fusion network. *Multimedia Tools and Applications*, 2022, vol. 81, no. 23, pp. 33051–33065.
26. Li Y., Chen C.L.P., Zhang T. A survey on Siamese network: methodologies, applications, and opportunities. *IEEE Transactions on Artificial Intelligence*, 2022, vol. 3, no. 6, pp. 994–1014.
27. Latif S.A., Sidek K.A., Hashim A.H.A. Hybrid CNN-ViT integration into Siamese networks for robust iris biometric verification. *Bulletin of Electrical Engineering and Informatics*, 2025, vol. 14, no. 4, pp. 3101–3109.
28. GOST R 52633.5-2011. *Zashchita informatsii. Tekhnika zashchity informatsii. Avtomaticheskoe obuchenie neyrosetevykh preobrazovateley biometriya-kod dostupa* [Information protection. Information protection technique. Automatic training of neural network converters for biometrics-access code]. Moscow, Standartinform Publ., 2018 (in Russ.).
29. Zhou X., Kuijper A., Veldhuis R., Busch C. Quantifying privacy and security of biometric fuzzy commitment. 2011 International Joint Conference on Biometrics (IJCB), Washington, DC, USA, IEEE, 2011, pp. 1–8.
30. Kausar F. Iris based cancelable biometric cryptosystem for secure healthcare smart card. *Egyptian Informatics Journal*, 2021, vol. 22, no. 4, pp. 447–453.
31. Matveev I., Safonov I. From iris image to embedded code: system of methods. *Algorithms*, 2023, vol. 16, no. 2, art. 87.
32. Lin K.-C., Chen Y.-M. A high-security-level iris cryptosystem based on fuzzy commitment and soft reliability extraction. *IEEE Transactions on Dependable and Secure Computing*, 2024, vol. 21, no. 4, pp. 1770–1784.
33. Shukla A., Demarest L., Fuller B., Ahmad S., Manicke C., Russell A., Chen S. Fuzzy extractors are practical: cryptographic strength key derivation from the iris. Proc. of the 2025 ACM SIGSAC Conf. on Computer and Communications Security (CCS '25), Taipei, Taiwan, New York, ACM, 2025, pp. 3605–3619.
34. Schroff F., Kalenichenko D., Philbin J. FaceNet: a unified embedding for face recognition and clustering. 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, IEEE, 2015, pp. 815–823.
35. Wen Y., Zhang K., Li Z., Qiao Y. A discriminative feature learning approach for deep face recognition. Computer Vision – ECCV 2016. Proc. of the 14th European Conf., Amsterdam, The Netherlands, Cham, Springer, 2016, pp. 499–515.

Stanislav E. Shtuka

Student, Department of Information Security,
Far Eastern Federal University (FEFU)
10, Ajax, Russky Island, Vladivostok, Russia, 690922
ORCID: 0009-0007-0659-6166
Phone: +7-914-712-25-67
Email: stanislav.shtuka@mail.ru

Aleksey E. Borshevnikov

Senior Analyst,
Industrial Cryptosystems JSC (ProCSy JSC)
2B, bld. 1, Otrdnaya st., Moscow, Russia, 127273
ORCID: 0000-0002-7383-1820
Phone: +7-924-131-67-97
Email: borshevnikov.ae@dvfu.ru

Received: 29.05.2026.

Accepted: 12.08.2026.