УДК: 004.93'1 Вестник УрФО № 2(52) / 2024, с. 106–121

Панфилова И. Е., Ложников П. С. DOI: 10.14529/secur240211

ИССЛЕДОВАНИЕ ПРИМЕНИМОСТИ НЕЙРОСЕТЕВЫХ ПРЕОБРАЗОВАТЕЛЕЙ «БИОМЕТРИЯ-КОД» ДЛЯ ЗАДАЧИ ОБНАРУЖЕНИЯ АТАК НА БИОМЕТРИЧЕСКОЕ ПРЕДЪЯВЛЕНИЕ[1]

В статье рассматривается применение нейросетевых преобразователей «биометрия-код» (НПБК) для защиты блоков обнаружения спуфинг-атак (атак на биометрическое предъявление) в системах биометрической аутентификации по лицу. Введение эффективных антиспуфинг методов имеет критическое значение для повышения надежности биометрических систем, однако внедрение таких методов может создать новые уязвимости. Предложенное решение основано на интеграции НПБК с глубокой нейронной сетью для осуществления бинарной классификации входных изображений лиц на реальные и поддельные. Это обеспечивает безопасное связывание биометрических данных с криптографическими ключами, снижая вероятность несанкционированного доступа. Экспериментальные результаты, полученные на наборе данных CelebA-Spoof, демонстрируют высокую точность работы модуля (97,2%) и низкий уровень средней ошибки классификации (ACER = 2,9%), что подтверждает эффективность предложенного подхода в обеспечении высокой защищенности процедуры аутентификации.

Ключевые слова: *нейросетевые преобразователи, глубокие нейронные сети, атака на биометрическое предъявление, спуфинг атака, распознавание лиц, биометрическая аутентификация.*

[1] Исследование выполнено при финансовой поддержке Минцифры России (Грант ИБ), проект № 40469-18/23-К

AN INVESTIGATION THE APPLICATION OF FUZZY NEURAL EXTRACTORS FOR FACE ANTI-SPOOFING

The article discusses the application of fuzzy neural extractors to protect spoofing attack detection units in facial biometric authentication systems. The introduction of effective anti-spoofing techniques is critical to improve the reliability of biometric systems, but the implementation of such techniques may create new vulnerabilities. The proposed solution is based on the integration of fuzzy neural extractors with a deep neural network to perform binary classification of input face images into real and spoofed ones. This provides secure binding of biometric data with cryptographic keys, reducing the probability of unauthorized access. Experimental results obtained on the CelebA-Spoof dataset demonstrate high accuracy of the module (97.2%) and low level of average classification error (ACER = 2.9%), which confirms the effectiveness of the proposed approach in ensuring high security of the authentication procedure.

Keywords: *neural network converters, deep neural networks, biometric presentation attack, spoofing attack, face recognition, biometric authentication..*

Введение

Системы распознавания лиц представляют собой технологические решения, способные идентифицировать и/или верифицировать личность человека с помощью его лицевых характеристик. Эти системы нашли широкое применение в различных областях, таких как финансы, безопасность, здравоохранение и информационные технологии. Несмотря на высокую степень надёжности систем биометрической аутентификации по лицу, они подвержены угрозам, связанным с подделкой биометрических данных – спуфинг атакам или атакам на биометрическое предъявление (согласно ГОСТ Р 58624.1-2019 [1]). Разработка и внедрение эффективных методов противодействия спуфинг атакам имеет критическое значение для обеспечения доверия к биометрическим системам аутентификации и защиты конфиденциальной информации (персональных данных пользователей).

Современные исследования в области антиспуфинга направлены на создание алгоритмов, способных надёжно классифицировать реальные и поддельные лица, используя передовые технологии глубокого обучения. Однако добавление решений антиспуфинга в системы биометрической аутентификации по лицу способны спровоцировать появление новых уязвимостей системы распознавания: на этапе обнаружения поддельных изображений может быть осуществлена кража биометрического шаблона. В этой связи, применение методов защиты биометрических шаблонов (ЗБШ) для модулей (систем) антиспуфинга является новой и нетривиальной исследовательской задачей [38].

Основной целью методов ЗБШ является защита биометрических шаблонов (уникальных физиологических характеристик человека, представленных в виде вектора) от несанкционированного доступа, подделки и компрометации. Современные исследователи [34] среди прочих выделяют три группы методов защиты биометрических шаблонов: отменяемая биометрия [35], биометрические криптосистемы [36] и гомоморфное шифрование [37]. Несмотря на характерные для каждой из групп достоинства, биометрические криптосистемы демонстрируют ряд существенных преимуществ перед методами отменяемой биометрии и гомоморфного шифрования. Биометрические криптосистемы используют криптографические ключи, связанные с биометрическими данными, что значительно снижает уязвимость системы к атакам. В случае утечки данных, криптографические

ключи можно изменить без необходимости повторного сбора биометрических данных. В отличие от отменяемой биометрии, где трансформации могут быть обратимыми и, следовательно, потенциально уязвимыми к атакам, биометрические криптосистемы обеспечивают более высокий уровень защиты за счёт сложности восстановления исходных данных из зашифрованных шаблонов. В сравнении с гомоморфным шифрованием, биометрические криптосистемы могут предложить более простую и менее ресурсоёмкую защиту, так как гомоморфное шифрование требует значительных вычислительных мощностей для обработки зашифрованных данных.

Одним из вариантов биометрических криптосистем, сочетающих в себе достоинства отменяемой биометрии и классических криптографических методов, являются схемы, обладающие возможностью связывания внешнего криптографического ключа с биометрическим образом [34]. К таким схемам относятся нейросетевые преобразователи «биометрия-код» (НПБК) [21], исключающие недостатки реализаций нечетких экстракторов [22] и обладающие возможностью анализа биометрических данных наравне с алгоритмами искусственного интеллекта. Основная цель НПБК — обеспечить надежное связывание биометрических данных с криптографическими ключами, которые затем используются для аутентификации и идентификации пользователей. Самой простой реализацией НПБК является преобразователь, обученный в соответствии с ГОСТ Р 52633.5-2011 [14], так называемый, классический НПБК. За счет своей уникальной структуры (широкой нейронной сети) такой НПБК способен обучаться на малых выборках биометрических образов, обогащая их в процессе обучения. Результатом обучения становятся высокие показатели точности распознавания биометрических образов и надежности процедуры аутентификации. Кроме того, согласно последним исследованиям [50], обозначенные показатели можно заметно улучшить за счет работы НПБК совместно с глубокими нейронными сетями, используемыми в качестве экстракторов признаков. Однако вопросы применимости таких реализаций для защиты альтернативных модулей систем биометрической аутентификации по лицу по-прежнему остаются не изученными.

Обзор существующих методов противодействия лицевым спуфинг атакам на основе глубокого обучения

Спуфинг атаки представляют собой вариант обмана биометрических систем аутентификации, при котором поддельные биометрические данные выдаются за подлинные с целью получения несанкционированного доступа. В контексте систем распознавания лиц, спуфинг атаки могут включать использование фотографий (распечатанных или демонстрируемых с цифровых устройств), видеозаписей, 3D-масок (распечатанных, силиконовых и т.д.) и других искусственных репрезентаций лица целевого пользователя. Для противодействия спуфинг атакам в системах распознавания лиц применяются различные методы, направленные на проверку подлинности представленных биометрических данных. Часто такие методы объединяют под общим термином liveness detection (методы определения живости), так как их главной задачей является ответ на вопрос «это живой (реальный) человек?». Отличать живые лица от подделок сегодня позволяют такие методы, как анализ текстуры кожи и изображений [29], наблюдение за микродвижениями [30, 31] (моргание или поворот головы), а также использование камер со специальными сенсорами [32].

Однако с появлением методов глубокого обучения (МГО) задача определения живого присутствия перестала быть трудоемким процессом, сопряжённым с ручным извлечением признаков поддельных изображений, характерных для традиционных методов liveness detection (LBP [5], SIFT [6], SURF [7], DoG [8], HOG [9] и другие). Теперь глубокие нейронные сети (ГНС) могут самостоятельно обнаруживать релевантные признаки, включая текстурные и контекстуальные особенности изображений настоящих и поддельных лиц. Кроме того, ГНС могут быть дополнительно улучшены методами регуляризации и предобучением на больших наборах данных, что увеличивает их способность к обобщению и устойчивости к различным типам атак.

Уже в 2014 году, авторы исследования [25] предложили первое полноценное решение систем определения живого присутствия на основе глубокого обучения с использованием 8-слойной неглубокой CNN для извлечения признаков. После этого до-

статочно часто стали появляться работы [26-28], в которых использовались уже предобученные глубокие модели (например, VGG16 или ResNet18), настраиваемые специально для задач определения живого присутствия с помощью трансферного обучения. Однако для того, чтобы оценить все разнообразие методов определения живого присутствия с помощью глубокого обучения, введем следующую классификацию таких методов [23]:

1. Гибридные методы: извлечение признаков с помощью классических методов с последующим применением глубоких моделей.

2. Традиционные методы обучения с учителем: так называемые end-to-end решения. Определение живого присутствия осуществляется путем применения методов глубокого обучения, чаще всего одной глубокой нейронной сети.

3. Методы, направленные на повышение обобщающей способности моделей глубокого обучения: подразумевают генерализацию моделей в отношении новых условий работы модели (освещение, качество изображения и др.) или новых типов атак.

4. Методы на основе дополнительной информации: используют специальные сенсоры или дополнительные модели для получения информации о входном изображении в иных диапазонах (инфракрасное излучение, тепловое излучение) или измерениях (карты глубины).

Наиболее простым вариантом обнаружения спуфинг атак с помощью метдов глубокого обучения является подход, при котором сначала извлекаются признаки из входных данных лица с помощью традиционных методов, а затем используется глубокое обучение для их семантического представления. Так, например, в работе [24] авторы используют LBP в качестве локальных дескрипторов, а затем работают с ними с помощью случайного леса. Стоит отметить, что исследователи не применяют CHC и при этом демонстрируют достаточно высокую эффективность на примере эталонного набора данных REPLAY-ATTACK [10]. Однако ключевым недостатком гибридных методов остается вся та же необходимость предварительного ручного извлечения признаков, свойственная традиционным подходам, а значит увеличение времени и ресурсов для обучения и настройки системы.

В большинстве работ, посвященных определению живого присутствия с использованием традиционных методов глубокого обучения, решение проблемы сводится к задаче бинарной классификации [39]. В таком случае модель обучается дифференцировать входные изображения по принципу «фальшивое лицо» (класс 1) и «реальное лицо» (класс 2). Такой подход является одним из наиболее простых и эффективных с точки зрения сходимости модели, однако не лишен недостатков: бинарная модель плохо поддается интерпретации, а выученные ею признаки сложно понять и использовать для улучшения производительности. Однако бинарная классификация способна демонстрировать довольно высокие результаты в случае учета временных характеристик распознавания (потока образов), что было продемонстрировано в работе [20] на примере модели FasTCo.

Отчасти с указанной проблемой способны справляться методы на основе попиксельного контроля (pixel-wise supervision) [4, 17, 19, 40] – подхода к обучению глубоких моделей, результатом которого становятся попиксельно маркированные изображения обучающего набора данных. Маркировка может осуществляться с целью получения карт псевдоглубины (pseudo depth labels) [17, 44], карт отражений (reflection maps) [45], карт бинарных масок (binary mask label) [46] или карт 3D облака точек (3D point cloud map) [47]. Идея получения таких различных карт при попиксельном контроле основывается на предположении о том, что подавляющее большинство спуфинг атак основаны на предъявлении системе двумерных изображений (распечаток или экранов устройств), в отличие от которых реальное лицо является объемным. Очевидно, что такой подход оказывается ограниченным с точки зрения работы с 3D атаками (масками), в связи с чем извлечение карт иного рода, например, карт бинарных масок [19], являются более предпочтительными для получения робастных моделей.

Одной из первых реализаций подхода стала архитектура DepthNet [2], до сих пор активно использующаяся для практических целей и работящая по принципу извлечения карт глубины (псевдоглубины) из входных изображений. Замена стандартных сверточных слоев DepthNet на специально разработанные для задачи антиспуфинга слои центральной разностной свертки (central

difference convolution (CDC)) позволили авторам работы [17] разработать новую архитектуру CDCN, демонстрирующую более высокие показатели точности распознавания спуфинг атак на протоколе №1 набора данных OULU-NPU [48] (ACER = 1.3%).

Однако высокие показатели метода попиксельного обучения на небольших наборах данных, вроде OULU-NPU [49] или SiW-M [49], трудно считать показательными, в особенности после появления одного из самых масштабных датасетов для задачи антиспуфинга – CelebA-Spoof [4]. Авторы коллекции утверждают, что одной из ключевых проблем развития моделей для обнаружения спуфинга являются наборы данных, плохо отражающие разнообразие спуфинг атак и их модификаций. С целью исправления ситуации был собран крупномасштабный набор данных и произведена качественная аннотация биометрических образов и атак. Дополнительно в работе [4] предложена одна из наиболее популярных моделей для задачи антиспуфинга AENet, за счет попиксельного обучения и механизмов внимания достигающая точности 99,6% на том же наборе данных.

Методы, направленные на повышение обобщающей способности моделей глубокого обучения, являются одними из самых перспективных среди современных подходов борьбы со спуфинг атаками. Актуальность направления связана с тем, что ГНС в принципе обладают слабой обобщающей способностью и часто «переучиваются» на специально подобранных наборах данных. Более того, согласно последним исследованиям [23], значительная часть работ по-прежнему опирается на небольшой пул устаревших наборов данных, которые трудно считать репрезентативными и пригодными для обучения моделей, предназначенных для работы в реальных условиях. В этом смысле показательными являются исследования, основанные на методах обучения с нулевым выстрелом (zero-shot learning) или с несколькими выстрелами (few-shot learning) [41], а также на методах обнаружения аномалий, в частности одноклассовой классификации. Так, например, в работе [15] авторы используют одноклассовый классификатор на основе многоканальной сверточной нейронной сети. Применение одноклассовой константной потери (one-class constative loss) для обучения классификатора позволило добиться однозначного разделения спуфинг образов и реальных изображений в пространстве векторных представлений. Такой подход обеспечивает возможность определения новых атак в реальных условиях. Аналогичного эффекта добиваются исследователи в работе [16], в качестве функции потерь использующие Hypersphere Loss Function. Применение функции позволяет добиться специфического распределения реальных образов в гиперсфере радиусом r и однозначно определять остальные образы как поддельные.

Наконец рассмотрим мультимодальный подход [42], применяющийся в настоящем исследовании и основанный на использовании дополнительной информации для обучения глубоких моделей. Основным достоинством подхода является возможность объединения информации из разных модальностей, что позволяет компенсировать недостатки каждой из них и дополнительно использовать различные алгоритмы и модели для анализа каждой из модальностей. Это позволяет оптимально использовать специализированные алгоритмы для обработки конкретного типа данных, улучшая общую производительность и точность системы. Кроме того, разные методы спуфинга могут быть направлены на уязвимости одной модальности, но крайне трудно обмануть систему, способную анализировать несколько модальностей одновременно.

Наиболее простым вариантом реализации подхода является использование специальных сенсоров для получения изображений в альтернативных диапазонах и обучение ГНС на полученных изображениях совместно со стандартными (RGB) [43]. Очевидны недостатки такого решения, связанные с необходимостью использования дополнительного оборудования. В связи с этим, дополнительной информацией для входов нейронной сети могут служить рассмотренные ранее карты, получаемые путем попиксельного контроля, например, карты псевдоглубины [3]. В данном случае неспособность карт глубины работать с 3D атаками частично компенсируется за счет дополнительного входа с классическим RGB изображением. Основной задачей для данного направления, в таком случае, становится поиск эффективных способов слияния информации от нескольких источников.

Из приведенного анализа видно, что наиболее перспективными методами противодействия спуфинг атакам в биометрических

системах аутентификации, в частности в системах распознавания лиц, являются методы на основе мультимодальных подходов и попиксельного контроля. Мультимодальные подходы позволяют объединять информацию из различных источников и биометрических модальностей, что компенсирует недостатки каждой из них и повышает общую точность и устойчивость системы к атакам. Методы попиксельного контроля, такие как карты псевдоглубины и отражений, обеспечивают детализированное представление изображений, что позволяет более эффективно различать реальные лица и подделки. Комбинирование этих методов может привести к созданию более робастных систем, способных противостоять различным видам атак, улучшая их производительность и надежность в реальных условиях.

Набор данных для экспериментальных исследований

Современные исследования в области лицевой биометрической аутентификации активно используют открытые наборы данных изображений и видеозаписей лиц для разработки и оценки алгоритмов определения подлинности лица. Специализированные наборы данных, такие как Replay-Attack [10], MSU-MFSD [11] и CelebA-Spoof [4], сфокусированы на задачах определения подлинности лиц и детекции спуфинг атак. Эти наборы данных включают изображения и видеозаписи различных атак, таких как использование фотографий, видео и 3D-масок. Наличие подобных специализированных наборов данных способствует возможности проведения экспериментальных оценок моделей глубокого обучения, направленных на выявление широкого спектра спуфинг атак.

Для проведения экспериментальных исследований, описанных ниже, за основу был взят один из немногих открытых наборов данных – CelebA-Spoof [4]. Набор данных CelebA-Spoof представляет собой обширную и тщательно аннотированную коллекцию изображений, специально созданную для задач анти-спуфинга в системах распознавания лиц. Датасет включает 625537 изображений 10177 субъектов, которые охватывают широкий спектр реальных лиц и различных типов атак, таких как атаки с использованием распечатанных изображений, атаки с использованием воспроизведения видео с различных устройств и распечатанные 3D маски. Каждое изображение в датасете сопровождается подробными аннотациями, включающими метки спуфинга (истинное или поддельное лицо), тип атаки (например, использование фотографий, видео или масок) и другие релевантные атрибуты. Изображения в датасете сделаны в различных условиях освещения, с разными позами и выражениями лиц.

Метрики оценки

В качестве основной метрики оценки работы предложенного решения используется точность распознавания (доля правильно классифицированных примеров относительно общего числа примеров). Для расчета указанной метрики использовалось следующее выражение:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

где TP (True Positives) — количество истинно положительных предсказаний, TN (True Negatives) — количество истинно отрицательных предсказаний, FP (False Positives) — количество ложно положительных предсказаний, FN (False Negatives) — количество ложно отрицательных предсказаний (когда модель ошибочно предсказала отрицательный класс).

В качестве дополнительной метрики высчитывается значение ACER (Average Classification Error Rate), являющееся общепринятой метрикой, использующейся для оценки общей производительности систем противодействия атакам на биометрическое предъявление и учитывающая ключевые ошибки – количество ложных принятий (APCER (Attack Presentation Classification Error Rate)) и ложных отказов (BPCER (Bona Fide Presentation Classification Error Rate)) – влияющие на надёжность системы.

$$ACER = \frac{APCER + BPCER}{2}$$

где $APCER = \frac{FP}{FP+TN}$, $BPCER = \frac{FN}{FN+TP}$.

Совместное использование указанных метрик обеспечивает всестороннюю оценку системы: высокое значение Accuracy указывает на общую эффективность классификации, тогда как низкое значение ACER свидетельствует о способности системы надежно различать реальные и поддельные образы.

Модуль обнаружения спуфинг атак для систем биометрической аутентификации по лицу

Для решения задачи обнаружения атак на биометрическое предъявление, при которой невозможен несанкционированный доступ к биометрическим данным пользователей, в настоящей работе предложен модуль обнаружения спуфинг атак для систем биометрической аутентификации по лицу с использованием нейросетевого преобразователя «биометрия-код».

Одним из способов нивелирования недостатков применения глубоких нейронных сетей для обнаружения спуфинг атак является логика разделения блока векторного представления образов и блока защиты биометрического шаблона (блока классификации) (рис. 1). Если в качестве последнего для классификации образов использовать широкие нейронные сети, способные обучаться автоматически (без применения градиентного спуска), то можно избежать переобучения всей сети на специальном наборе данных и несколько повысить обобщающую способность модели за счет классификатора, обученного общему представлению реальных и поддельных изображений. В таком случае, спектр атак, представленный в наборе данных CelebA-Spoof, не оказывает решающего значения при обучении и тестировании предложенных моделей.

Как отмечалось ранее, в качестве описанной широкой нейронной сети может выступать нейросетевой преобразователь «биометрия-код», позволяющий достигать сразу двух ключевых целей в разработке модуля обнаружения спуфинг атак: противодействие угрозам компрометации биометрических образов пользователей, проходящим через систему обнаружения, а также высокая точность классификации реальных и поддельных изображений лиц.

Дополнительным достоинством всего предложенного решения (модуля), является отсутствие необходимости полного повторного переобучения модели глубокого обучения (блока векторного представления), предшествующей НПБК, в случае компрометации биометрических образов лиц на этапе обнаружения спуфинг атак.

В рамках экспериментальной реализации модуля обнаружения спуфинг атак в качестве блока векторного представления была обучена глубокая нейронная сеть, основанная на архитектуре FeatherNet [3]. FeatherNet — это легковесная архитектура сверточной нейронной сети, разработанная для задачи обнаружения спуфинг атак в системах распознавания лиц. В основе архитектуры лежат идеи минимизации вычислительных затрат и параметров модели без потери точности.

Одной из ключевых особенностей оригинальной архитектуры FeatherNet, предложенной в работе [3], является замена широко применяемого для снижения размерности слоя глобального усредняющего пулинга (Global Average Pooling (GAP)) на так называемый модуль потоковой передачи данных (Streaming Module), основанный на глубинной свертке (depthwise convolution) с шагом > 1. С помощью такой замены удается избегать негативных последствий применения GAP для задач распознавания лиц, связанных с усреднением всех значений карт признаков вне зависимости от степени их «важности» для конкретного примера. Кроме того, FeatherNet является примером мультимодальных архитектур, прини-

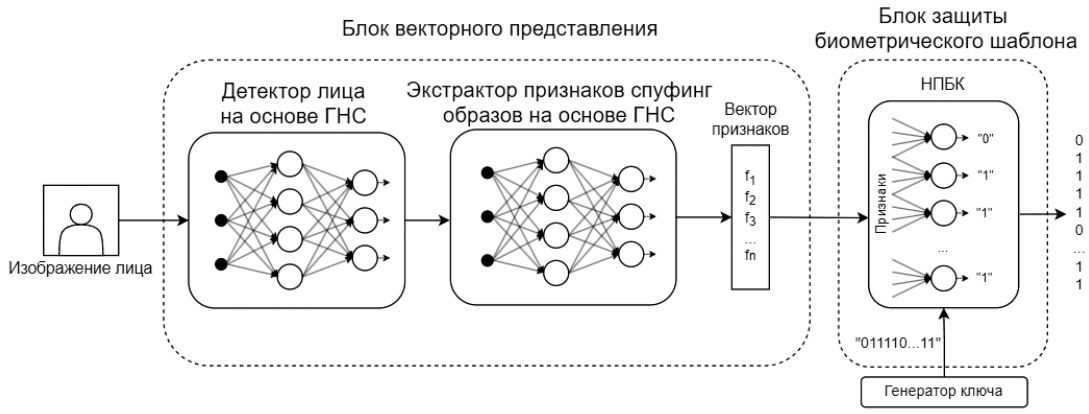

Рис. 1. Схема модуля обнаружения спуфинг атак для систем биометрической аутентификации по лицу

Таблица 1.

Архитектура модифицированной сверточной нейронной сети для извлечения признаков на основе FeatherNet

Назначение	Слой	Описание	Размерность выходного вектора
Усреднение мульти-модальных входных значений	conv1	Блок с Conv2d_cdcn (3 входных канала, 32 выходных, ядро 3x3, шаг 2), BatchNorm2d и Hardswish активацией.	32
	avgpool	AdaptiveAvgPool2d, выполняет адаптивное усреднение по размерам входного изображения для слоя layer1.	32
Извлечение признаков	layer1	Блоки, содержащие InvertedResidual блоки, включая Downsample, Conv2d, BatchNorm2d, Hardswish и SELayer (для некоторых блоков).	16
	layer2		32
	layer3		64
	layer4		96
Классификаторы («головы»)	fc_face	Блок с Dropout (вероятность отсева 0.15), BatchNorm1d, Hardswish и Linear (входных 96, выходных 40).	40
	fc_attack	Блок с Dropout (вероятность отсева 0.15), BatchNorm1d, Hardswish и Linear (входных 96, выходных 11).	11
	fc_light	Блок с Dropout (вероятность отсева 0.15), BatchNorm1d, Hardswish и Linear (входных 96, выходных 5).	5
	fc_live	Блок с Dropout (вероятность отсева 0.15), BatchNorm1d, Hardswish и AngleSimpleLinear (вычисление косинуса угла между векторами в пространстве признаков).	1
	depth	Блок с Conv2d (входных 96, выходных 1), Upsample (размер 14x14, метод 'bilinear') и Sigmoid активацией.	1

мающих на вход не только стандартные изображения (RGB), но и дополнительную информацию в виде карт глубины [44] и инфракрасных изображений лиц [42].

Для обучения описанной архитектуры и получения блока векторного представления (экстрактора признаков), способного дифференцировать признаки, полученные из изображений реальных и поддельных лиц, были произведены ряд модификаций в структуре сети FeatherNet (табл. 1). Целью модификаций является объединение преимуществ технологий попиксельного контроля (центральная разностная свертка) и мультимодальных архитектур для повышения эффективности работы итоговой модели в отношении разнообразия спуфинг атак.

В первую очередь, для обучения сети кроме стандартных RGB изображений использовались только карты глубины лиц, представленные во вспомогательном наборе данных CelebA-Spoof Depth Image [33]. Исключение изображений в инфракрасном диапазоне из процедуры обучения обосновано отсутствием таковых для экспериментального набора данных CelebA-Spoof.

В качестве дополнительных улучшений были произведены замены функций активаций ReLU (Rectified Linear Unit) на относительно новый тип нелинейности для обучения глубоких нейронных сетей HardSwish (h-swish), впервые представленный в рамках исследований архитектуры MobileNetV3 [18]:

$$hardswish(x) = x\frac{ReLU6(x+3)}{6}$$

где ReLU6 – это функция активации ReLU, ограниченная значением 6. HardSwish явля-

ется аппроксимацией swish, которая умножает входное значение x на сигмовидную функцию от этого же значения. Для современных архитектур, разработанных для мобильных и встраиваемых систем, использование функции активации HardSwish позволяет достигать высокого соотношения производительности и затрат.

Кроме того, для блока усреднения мультимодальных входных значений были изменены процедуры свертки, позволяющие извлекать пространственные признаки из входных данных: классическая 2D свертка (Conv2d) в настоящей работе заменяется на ее модификацию, предназначенную для улучшения способности модели извлекать локальные градиентные признаки в данных – central difference convolution (CDC) [17]. Центральная разностная свертка работает за счет добавления к процедуре стандартной свертки входного изображения с фильтром K дополнительной информации в виде разности каждого элемента окна свертки и центрального элемента этого окна, умноженной на соответствующий элемент фильтра. Добавление описанной модификации в первые слои усреднения позволяют повысить устойчивость модели к небольшим изменениям и искажениям в данных, что является критически важным для возможности распознавания максимально приближенных к реальности спуфинг атак.

Экспериментальная оценка предложенного решения

Для повышения обобщающей способности модели, а также предотвращения возможного переобучения была произведена аугментация данных тренировочного набора. Для этого входные изображения 7 видам дополнительных преобразований:

1. Добавление шума, имитирующего шум цифровых камер (ISOnoise), с определенным сдвигом цвета и интенсивностью. Применяется с вероятностью 5%.

2. Изменение яркости и контраста в заданных пределах. Применяется с вероятностью 12.5%.

3. Имитация движения, осуществляющее размытие, имитирующее движение, с ограничением размытия до 3 пикселей. Применяется с вероятностью 20%.

4. Имитация сжатия изображения, помогающее снижать его качество. Применяется с вероятностью 25%.

5. Случайное удаление фрагментов изображения (заполнение черным) в виде прямоугольных областей. Применяется с вероятностью 25%.

6. Добавление гауссовского шума. Применяется с вероятностью 20%.

7. Нормализация изображения с заданными средними значениями и стандартными отклонениями для каждого канала (RGB).

Применение указанных видов аугментации способно значительно повысить эффективность антиспуфинг систем распознавания лиц за счет увеличения разнообразия обучающих данных и повышения устойчивости моделей к различным искажениям. Добавление шума, изменение яркости и контраста, а также имитация движения и сжатия изображений способствуют адаптации моделей к вариативным условиям съемки и различным уровням качества изображений. Случайное удаление фрагментов изображения и добавление гауссовского шума увеличивают способность моделей справляться с частичными потерями информации и шумами. Нормализация изображений обеспечивает стабильность процесса обучения, выравнивая данные и ускоряя сходимость моделей.

Обучение модифицированной архитектуры FeatherNet осуществлялось на полном наборе данных CelebA-Spoof в течение 15 эпох с помощью функции потерь Cross Entropy для «головы» fc_live, осуществляющей бинарную классификацию реальных и поддельных изображений (рис. 2). Предварительно обучающие данные были разделены на тренировочную и тестовую (валидационную) выборки, каждая из которых случайным образом подвергалась аугментации в соответствии с описанными выше преобразованиями.

На вариационной выборке максимальное значение точности работы сети составило только 92,7%, несмотря на то, что значения точности на тренировочных данных превышают 97%. Для дальнейшего использования обученной сети в качестве экстрактора признаков, слои классификатора «замораживались», а работа осуществлялась с 96-мерным вектором признаков на выходе предшествующего классификатору слоя.

В качестве детектора лиц на входных изображениях использовалась предобученная на крупномасштабном наборе данных WIDERFACE [12] модель RetinaFace [13]. Модель разработана для одностадийного обнаружения лиц с высокой точностью и использует стратегии многозадачного обучения.

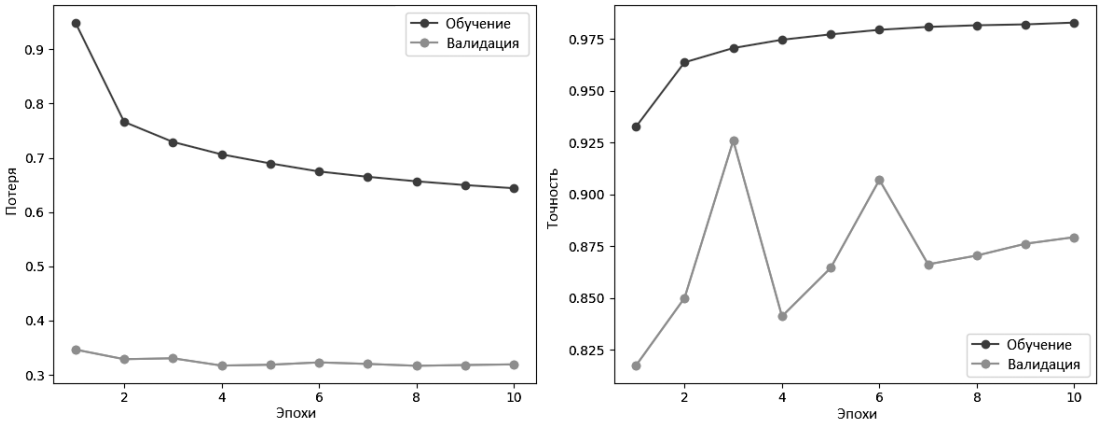

Рис. 2. Результаты обучения модифицированной архитектуры FeatherNet

В качестве классификатора реальных и поддельных входных образов лиц реализован нейросетевой преобразователь биометрия-код, процедура обучения которого представлена в ГОСТ Р 52633.5-2011. Адаптация логики работы НПБК под задачу бинарной классификации осуществляется путем построения преобразователя для реальных изображений лиц (класс C_1). В таком случае, поддельные изображения (класс C_2) расцениваются НПБК как «Чужие», а случайный код на выходе свидетельствует о решении в пользу класса C_2. Принадлежность классу C_i, $i = 1, 2$, оценивается исходя из получаемого на выходе НПБК бинарного кода (ключ K_2 в случае класса C_1). Особенностью построения НПБК в качестве классификатора является допущение о возможности дублировании входов нейрона в связи с отсутствием необходимости сокрытия структуры преобразователя. Для оценки качества осуществляемой бинарной классификации i-ого входного образа применяется следующее правило:

$$\begin{cases} (\bar{a}_i \in C_1 \ \wedge \ h_i < \ threshold) \rightarrow \ TP \\ (\bar{a}_i \in C_1 \ \wedge \ h_i > \ threshold) \rightarrow \ FN \\ (\bar{a}_i \in C_2 \ \wedge \ h_i < \ threshold) \rightarrow \ FP \\ (\bar{a}_i \in C_2 \ \wedge \ h_i > \ threshold) \rightarrow \ TN \end{cases}$$

где h_i – i-ое значение расстояния Хэмминга между ожидаемым кодом и выходом НПБК, $threshold$ – порог, определяющий допустимое количество ошибок в коде i-ого входного образа для корректного отнесения его к одной из групп классифицированных образов: TP – True Positive, FN – False Negative, FP – False Positive или TN – True Negative. Полученный классификатор не требует итерационного обучения (осуществляется автоматически) и большого числа обучающих примеров.

Итоговый эксперимент по оценке точности работы нейросетевого преобразователя «биометрия-код» в качестве классификатора (рис. 3)

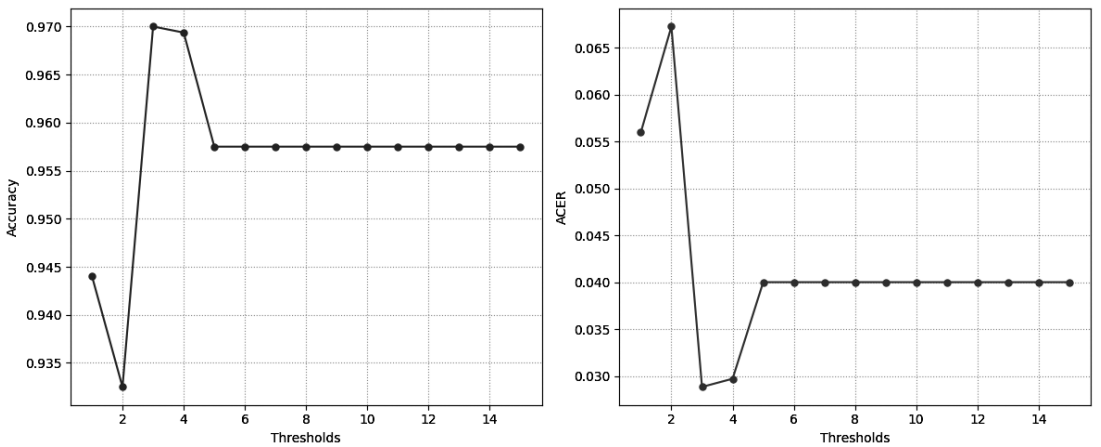

Рис. 3. Точность (accuracy) работы НПБК при разных значениях threshold

проводился с помощью специально подготовленных для этой задачи выборок (тренировочной и тестовой) из датасета CelebA-Spoof. В случае обучающей выборки случайным образом из классов (субъектов) основного набора данных выбирались 100 изображений реальных лиц, представляющих собой класс C_1, и 100 изображений поддельных лиц, представляющих собой разнообразные атаки исходного набора данных CelebA-Spoof (класс C_2). Аналогичная процедура была произведена для получения тестовой выборки, однако полученные 200 изображений дополнительно случайным образом перемешивались.

Анализ результатов работы НПБК при различных значениях threshold (рис. 3) продемонстрировал, что оптимальное значение порога, при котором достигается наивысшая точность (97.0%) и минимальная среднеклассовая ошибка (ACER = 2.9%) составляет threshold = 3. Это значение обеспечивает наилучшую производительность модели в задаче классификации реальных и поддельных биометрических данных. При других значениях порога наблюдается снижение точности до уровня около 95.5% и увеличение ACER, особенно при threshold = 2, где ошибка превышает 6.5%, что свидетельствует о значительном ухудшении качества классификации. Таким образом, пороговое значение threshold = 3 обеспечивает наилучшее соотношение между точностью распознавания и надежностью работы модуля, а также является наиболее оптимальным для задачи классификации реальных и поддельных биометрических лицевых данных.

Сравнение предложенного решения с существующими аналогами на основе глубокого обучения

Результаты сравнения предложенного решения с классическими моделями глубокого обучения, используемыми для задачи обнаружения спуфинг атак, представлены в таблице 2. Несмотря на то, что в части исследований [15, 17, 19, 20] авторы не предоставляют информации о результирующей точности работы сети, оценку моделей можно производить исходя из метрики ACER.

Из таблицы видно, что разработанный модуль (FeatherNet + НПБК) демонстрирует точность 97,2%, что уступает только модели AENet (99,6%), однако по-прежнему показывает высокий уровень распознавания реальных и поддельных лиц. В свою очередь, значение ACER для предложенного решения составляет 2,9%, что ниже, чем у AENet (3,09%) и значительно ниже по сравнению с моделями DeepPixBiS (5,97%) и CDCN++ (1,3%). Такие показатели ACER свидетельствуют о достаточно высокой надежности модели при условии обеспечения безопасного режима работы антиспуфинг модуля.

Показатели ACER для моделей MCCNN (BCE+OCCL)-GMM и FasTCo на наборе данных SiW-M демонстрируют большую вариативность (14.9 ± 7.8% и 10.1 ± 5.6% соответственно), что указывает на их меньшую стабильность по сравнению с FeatherNet + НПБК, а также на тот факт, что глубокие нейронные сети для обнаружения спуфинг атак, зачастую, проучиваются на специализированных наборах данных и показатели их эффективности, полученные в результате обучения, мо-

Таблица 2.

Сравнительные результаты работы предложенного решения с моделями глубокого обучения для обнаружения спуфинг атак

№	Модель	Набор данных	Accuracy	ACER
1	DeepPixBiS [19]	OULU-NPU (p.2)	-	5.97%
2	CDCN++ [17]	OULU-NPU (p.1)	-	1.3%
3	AENet [4]	CelebA-Spoof Dataset	99,60%	3.09%
4	MCCNN (BCE+OCCL)-GMM [15]	SiW-M	-	14.9 ± 7.8%
5	FasTCo [20]	SiW-M	-	10.1 ± 5.6%
7	FeatherNet + НПБК	CelebA-Spoof Dataset	97,20%	2,90%

гут существенно отличатся от значений, полученных в реальных условиях функционирования системы.

Несмотря на сравнительно невысокие показатели точности работы НПБК в качестве классификатора, сохраняется ключевое преимущество предложенного решения: безопасная реализация биометрической аутентификации по лицу, при которой модуль обнаружения спуфинг атак перестает быть точкой потенциальных уязвимостей. По-видимому, применение методов защиты биометрических шаблонов лиц к решениям для обнаружения спуфинг атак может привести к снижению точности распознавания, но взамен значительно повышает безопасность процедуры аутентификации с интегрированными модулями антиспуфинга.

Заключение

Настоящая работа посвящена исследованию применимости нейросетевых преобразователей «биометрия-код» для защиты блоков обнаружения спуфинг атак в системах биометрической аутентификации по лицу. С этой целью разработан и предложен антиспуфинг модуль на основе НПБК и глубокой нейронной сети, осуществляющий бинарную классификацию входных образов лиц на реальные и поддельные изображения. За счет разделения блока векторного представления образов (глубокой нейронной сети) и блока принятия решения в виде классификатора на основе НПБК, повышается обобщающая способность предложенного решения по отношению к разнообразию реализации спуфинг атак и решается проблема несанкционированного доступа в системах биометрической аутентификации по лицу, осуществляемого через блоки обнаружения спуфинг атак. Лучшее значение точности работы модуля на наборе данных CelebA-Spoof составило 97,2% (ACER = 2,9%), что говорит о приемлемом уровне производительности решения при высоком уровне защищенности процедуры аутентификации.

Литература

1. ГОСТ Р 58624.1-2019. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура – Введ. 01.06.2020. – М.: Стандарт информ, 2019. – 11 с. – (Система стандартов по информации, библиотечному и издательскому делу).

2. Y. Atoum, Y. Liu, A. Jourabloo, and X. Liu, "Face anti-spoofing using patch and depth-based CNNs," in Proc. IEEE Int. Joint Conf. Biometrics, 2017, pp. 319–328.

3. Zhang P. et al. FeatherNets: Convolutional neural networks as light as feather for face anti-spoofing //Proceedings of the IEEE/CVF conference on computer vision and pattern recognition workshops. – 2019. – С. 0-0.

4. Zhang Y. et al. Celeba-spoof: Large-scale face anti-spoofing dataset with rich annotations // Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part XII 16. – Springer International Publishing, 2020. – С. 70-85.

5. Das, D., & Chakraborty, S. Face liveness detection based on frequency and micro-texture analysis // 2014 International Conference on Advances in Engineering & Technology Research (ICAETR), 2014.

6. Patel, K., Han, H., & Jain, A. K. Secure Face Unlock: Spoof Detection on Smartphones // IEEE Transactions on Information Forensics and Security, 11(10), 2016.

7. Boulkenafet, Z., Komulainen, J., & Hadid, A. Face Anti-Spoofing using Speeded-Up Robust Features and Fisher Vector Encoding // IEEE Signal Processing Letters, 2016.

8. Tan, X., Li, Y., Liu, J., & Jiang, L. Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model // Lecture Notes in Computer Science, 2010.

9. Komulainen, J., Hadid, A., & Pietikainen, M. Context based face anti-spoofing // 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013.

10. Chingovska I., Anjos A., Marcel S. On the effectiveness of local binary patterns in face anti-spoofing //2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG). – IEEE, 2012. – С. 1-7.

11. Wen D., Han H., Jain A. K. Face spoof detection with image distortion analysis //IEEE Transactions on Information Forensics and Security. – 2015. – Т. 10. – №. 4. – С. 746-761.

12. Yang S. et al. Wider face: A face detection benchmark //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2016. – С. 5525-5533.

13. Deng J. et al. Retinaface: Single-stage dense face localisation in the wild //arXiv preprint arXiv:1905.00641. – 2019.

14. ГОСТ Р 52633.5-2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа – Введ. 01.04.2012. – М.: Стандарт информ, 2018. – 13 с. – (Система стандартов по информации, библиотечному и издательскому делу).

15. George, Anjith, and Sébastien Marcel. "Learning one class representations for face presentation attack detection using multi-channel convolutional neural networks." IEEE Transactions on Information Forensics and Security 16 (2020): 361-375.

16. Li, Zhi, et al. "Unseen face presentation attack detection with hypersphere loss." ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2020.

17. Yu Z. et al. Searching central difference convolutional networks for face anti-spoofing //Proceedings of the IEEE/CVF conference on computer vision and pattern recognition. – 2020. – С. 5295-5305.

18. Howard A. et al. Searching for mobilenetv3 //Proceedings of the IEEE/CVF international conference on computer vision. – 2019. – С. 1314-1324.

19. George A., Marcel S. Deep pixel-wise binary supervision for face presentation attack detection //2019 International Conference on Biometrics (ICB). – IEEE, 2019. – С. 1-8.

20. Xu X., Xiong Y., Xia W. On improving temporal consistency for online face liveness detection system //Proceedings of the IEEE/CVF International Conference on Computer Vision. – 2021. – С. 824-833.

21. B. S. Akhmetov, A. I. Ivanov, and Z. Alimseitova, 'Training of neural network biometry-code converters', News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, vol. 1, pp. 61–68, Jan. 2018.

22. Sarkar, A., & Singh, B. K. (2020). A review on performance, security and various biometric template protection schemes for biometric authentication systems. Multimedia Tools and Applications

23. Zitong Yu, Yunxiao Qin, Xiaobai Li, Chenxu Zhao, Zhen Lei, Guoying Zhao. Deep Learning for Face Anti-Spoofing: A Survey // IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2022.

24. R. Cai and C. Chen. Learning deep forest with multi-scale local binary pattern features for face anti-spoofing // arXiv preprint, 2019.

25. J. Yang, Z. Lei, and S. Z. Li. Learn convolutional neural network for face anti-spoofing // arXiv preprint, 2014.

26. O. Lucena, A. Junior, V. Moia, R. Souza, E. Valle, and R. Lotufo. Transfer learning using convolutional neural networks for face anti-spoofing // ICIAR, 2017.

27. H. Chen, G. Hu, Z. Lei, Y. Chen, N. M. Robertson, and S. Z. Li. Attention-based two-stream convolutional networks for face spoofing detection // TIFS, 2019.

28. A. George and S. Marcel. On the effectiveness of vision transformers for zero-shot face anti-spoofing // arXiv preprint, 2020.

29. I Chingovska, A Anjos, Sébastien Marcel. On the Effectiveness of Local Binary Patterns in Face Anti-spoofing // IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2012.

30. Anjos, A., Chakka, M. M., & Marcel, S. Motion-based counter-measures to photo attacks in face recognition // IET Biometrics, 3(3), 2014.

31. G. Pan, L. Sun, Z. Wu, and S. Lao. Eyeblink-based anti-spoofing in face recognition from a generic webcamera // ICCV, 2007.

32. 32. Mohamed, S., Ghoneim, A., & Youssif, A. Visible/Infrared face spoofing detection using texture descriptors // MATEC Web of Conferences, 2019.

33. 33. Kaggle. CelebA-Spoof Depth Image. Available at: https://www.kaggle.com/datasets/attentionlayer241/celeba-spoof-depth-image (accessed 1 August 2024).

34. Sarkar A., Singh B. K. A review on performance, security and various biometric template protection schemes for biometric authentication systems //Multimedia Tools and Applications. – 2020. – Т. 79. – №. 37. – С. 27721-27776.

35. Manisha, Kumar N. Cancelable biometrics: a comprehensive survey //Artificial Intelligence Review. – 2020. – Т. 53. – №. 5. – С. 3403-3446.

36. Kaur P., Kumar N., Singh M. Biometric cryptosystems: a comprehensive survey //Multimedia Tools and Applications. – 2023. – Т. 82. – №. 11. – С. 16635-16690.

37. Bassit A. et al. Hybrid biometric template protection: Resolving the agony of choice between bloom filters and homomorphic encryption //IET biometrics. – 2022. – Т. 11. – №. 5. – С. 430-444.

38. Song, Baogang, et al. "An Investigation of the Effectiveness of Template Protection Methods on Protecting Privacy During Iris Spoof Detection." Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data. Singapore: Springer Nature Singapore, 2023.

39. Yang, Jianwei, Zhen Lei, and Stan Z. Li. "Learn convolutional neural network for face anti-spoofing." arXiv preprint arXiv:1408.5601 (2014).

40. Y. Qin, Z. Yu, L. Yan, Z.Wang, C. Zhao, and Z. Lei, "Meta-teacher for face anti-spoofing," TPAMI, 2021.

41. Y. Qin, C. Zhao, X. Zhu, Z. Wang, Z. Yu, T. Fu, F. Zhou, J. Shi, and Z. Lei, "Learning meta model for zero- and few-shot face anti-spoofing," in AAAI, 2020.

42. A. George and S. Marcel, "Cross modal focal loss for rgbd face anti-spoofing," in CVPR, 2021.

43. A. Liu, Z. Tan, J. Wan, Y. Liang, Z. Lei, G. Guo, and S. Z. Li, "Face anti-spoofing via adversarial cross-modality translation," TIFS, 2021.

44. D. Peng, J. Xiao, R. Zhu, and G. Gao, "Ts-fen: Probing feature selection strategy for face anti-spoofing," in ICASS. IEEE, 2020.

45. Z. Yu, X. Li, X. Niu, J. Shi, and G. Zhao, "Face anti-spoofing with human material perception," in ECCV, 2020.

46. A. George and S. Marcel, "Deep pixel-wise binary supervision for face presentation attack detection," in ICB, no. CONF, 2019.

47. X. Li, J. Wan, Y. Jin, A. Liu, G. Guo, and S. Z. Li, "3dpc-net: 3d point cloud network for face anti-spoofing," 2020.

48. Boulkenafet Z. et al. OULU-NPU: A mobile face presentation attack database with real-world variations //2017 12th IEEE international conference on automatic face & gesture recognition (FG 2017). – IEEE, 2017. – С. 612-618.

49. Liu Y., Jourabloo A., Liu X. Learning deep models for face anti-spoofing: Binary or auxiliary supervision //Proceedings of the IEEE conference on computer vision and pattern recognition. – 2018. – С. 389-398.

50. Sulavko A. Biometric-based key generation and user authentication using acoustic characteristics of the outer ear and a network of correlation neurons //Sensors. – 2022. – Т. 22. – №. 23. – С. 9551.

References

1. ГОСТ Р 58624.1-2019. Informatsionnye tekhnologii. Biometriya. Obnaruzhenie ataki na biometricheskoe pred"yavlenie. Chast' 1. Struktura – Vved. 01.06.2020. – M.: Standart inform, 2019. – 11 s. – (Sistema standartov po informatsii, bibliotechnomu i izdatel'skomu delu).

2. Atoum Y., Liu Y., Jourabloo A., Liu X. Face Anti-Spoofing Using Patch and Depth-Based CNNs. In: Proc. IEEE Int. Joint Conf. Biometrics, 2017, pp. 319–328.

3. Zhang P. et al. FeatherNets: Convolutional Neural Networks as Light as Feather for Face Anti-Spoofing. In: Proc. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, 2019, pp. 0-0.

4. Zhang Y. et al. Celeba-Spoof: Large-Scale Face Anti-Spoofing Dataset with Rich Annotations. In: Computer Vision – ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part XII 16, Springer International Publishing, 2020, pp. 70-85.

5. Das D., Chakraborty S. Face Liveness Detection Based on Frequency and Micro-Texture Analysis. In: 2014 International Conference on Advances in Engineering & Technology Research (ICAETR), 2014.

6. Patel K., Han H., Jain A.K. Secure Face Unlock: Spoof Detection on Smartphones. In: IEEE Transactions on Information Forensics and Security, 2016, vol. 11, no. 10.

7. Boulkenafet Z., Komulainen J., Hadid A. Face Anti-Spoofing Using Speeded-Up Robust Features and Fisher Vector Encoding. In: IEEE Signal Processing Letters, 2016.

8. Tan X., Li Y., Liu J., Jiang L. Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model. In: Lecture Notes in Computer Science, 2010.

9. Komulainen J., Hadid A., Pietikainen M. Context Based Face Anti-Spoofing. In: 2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS), 2013.

10. Chingovska I., Anjos A., Marcel S. On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. In: 2012 BIOSIG-proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG), IEEE, 2012, pp. 1-7.

11. Wen D., Han H., Jain A.K. Face Spoof Detection with Image Distortion Analysis. In: IEEE Transactions on Information Forensics and Security, 2015, vol. 10, no. 4, pp. 746-761.

12. Yang S. et al. Wider Face: A Face Detection Benchmark. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 5525-5533.

13. Deng J. et al. RetinaFace: Single-Stage Dense Face Localisation in the Wild. In: arXiv preprint arXiv:1905.00641, 2019.

14. ГОСТ Р 52633.5-2011. Zashchita informatsii. Tekhnika zashchity informatsii. Avtomaticheskoe obuchenie neiurosetevykh preobrazovatelei biometriya-kod dostupa – Vved. 01.04.2012. – M.: Standart inform, 2018. – 13 s. – (Sistema standartov po informatsii, bibliotechnomu i izdatel'skomu delu).

15. George A., Marcel S. Learning One Class Representations for Face Presentation Attack Detection Using Multi-Channel Convolutional Neural Networks. In: IEEE Transactions on Information Forensics and Security, 2020, vol. 16, pp. 361-375.

16. Li Z. et al. Unseen Face Presentation Attack Detection with Hypersphere Loss. In: ICASSP 2020-2020 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), IEEE, 2020.

17. Yu Z. et al. Searching Central Difference Convolutional Networks for Face Anti-Spoofing. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 5295-5305.

18. Howard A. et al. Searching for MobileNetV3. In: Proceedings of the IEEE/CVF International Conference on Computer Vision, 2019, pp. 1314-1324.

19. George A., Marcel S. Deep Pixel-Wise Binary Supervision for Face Presentation Attack Detection. In: 2019 International Conference on Biometrics (ICB), IEEE, 2019, pp. 1-8.

20. Xu X., Xiong Y., Xia W. On Improving Temporal Consistency for Online Face Liveness Detection System. In: Proceedings of the IEEE/CVF International Conference on Computer Vision, 2021, pp. 824-833.

21. Akhmetov B.S., Ivanov A.I., Alimseitova Z. Training of Neural Network Biometry-Code Converters. In: News of the National Academy of Sciences of the Republic of Kazakhstan, Series of Geology and Technical Sciences, 2018, vol. 1, pp. 61–68.

22. Sarkar A., Singh B.K. A Review on Performance, Security and Various Biometric Template Protection Schemes for Biometric Authentication Systems. In: Multimedia Tools and Applications, 2020.

23. Yu Z., Qin Y., Li X., Zhao C., Lei Z., Zhao G. Deep Learning for Face Anti-Spoofing: A Survey. In: IEEE Transactions on Pattern Analysis and Machine Intelligence (TPAMI), 2022.

24. Cai R., Chen C. Learning Deep Forest with Multi-Scale Local Binary Pattern Features for Face Anti-Spoofing. In: arXiv preprint, 2019.

25. Yang J., Lei Z., Li S.Z. Learn Convolutional Neural Network for Face Anti-Spoofing. In: arXiv preprint, 2014.

26. Lucena O., Junior A., Moia V., Souza R., Valle E., Lotufo R. Transfer Learning Using Convolutional Neural Networks for Face Anti-Spoofing. In: ICIAR, 2017.

27. Chen H., Hu G., Lei Z., Chen Y., Robertson N.M., Li S.Z. Attention-Based Two-Stream Convolutional Networks for Face Spoofing Detection. In: TIFS, 2019.

28. George A., Marcel S. On the Effectiveness of Vision Transformers for Zero-Shot Face Anti-Spoofing. In: arXiv preprint, 2020.

29. Chingovska I., Anjos A., Marcel S. On the Effectiveness of Local Binary Patterns in Face Anti-Spoofing. In: IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), 2012.

30. Anjos A., Chakka M.M., Marcel S. Motion-Based Counter-Measures to Photo Attacks in Face Recognition. In: IET Biometrics, 2014, vol. 3, no. 3.

31. Pan G., Sun L., Wu Z., Lao S. Eyeblink-Based Anti-Spoofing in Face Recognition from a Generic Webcamera. In: ICCV, 2007.

32. Mohamed S., Ghoneim A., Youssif A. Visible/Infrared Face Spoofing Detection Using Texture Descriptors. In: MATEC Web of Conferences, 2019.

33. Kaggle. CelebA-Spoof Depth Image. Available at: https://www.kaggle.com/datasets/attentionlayer241/celeba-spoof-depth-image (accessed 1 August 2024).

34. Sarkar A., Singh B.K. A Review on Performance, Security and Various Biometric Template Protection Schemes for Biometric Authentication Systems. In: Multimedia Tools and Applications, 2020, vol. 79, no. 37, pp. 27721-27776.

35. Manisha, Kumar N. Cancelable Biometrics: A Comprehensive Survey. In: Artificial Intelligence Review, 2020, vol. 53, no. 5, pp. 3403-3446.

36. Kaur P., Kumar N., Singh M. Biometric Cryptosystems: A Comprehensive Survey. In: Multimedia Tools and Applications, 2023, vol. 82, no. 11, pp. 16635-16690.

37. Bassit A. et al. Hybrid Biometric Template Protection: Resolving the Agony of Choice between Bloom Filters and Homomorphic Encryption. In: IET Biometrics, 2022, vol. 11, no. 5, pp. 430-444.

38. Song B. et al. An Investigation of the Effectiveness of Template Protection Methods on Protecting Privacy During Iris Spoof Detection. In: Asia-Pacific Web (APWeb) and Web-Age Information Management (WAIM) Joint International Conference on Web and Big Data, Singapore: Springer Nature Singapore, 2023.

39. Yang J., Lei Z., Li S.Z. Learn Convolutional Neural Network for Face Anti-Spoofing. In: arXiv preprint arXiv:1408.5601, 2014.

40. Qin Y., Yu Z., Yan L., Wang Z., Zhao C., Lei Z. Meta-Teacher for Face Anti-Spoofing. In: TPAMI, 2021.

41. Qin Y. et al. Learning Meta Model for Zero-and Few-Shot Face Anti-Spoofing. In: AAAI, 2020.

42. George A., Marcel S. Cross Modal Focal Loss for RGBD Face Anti-Spoofing. In: CVPR, 2021.

43. Liu A. et al. Face Anti-Spoofing via Adversarial Cross-Modality Translation. In: TIFS, 2021.

44. Peng D. et al. TS-FEN: Probing Feature Selection Strategy for Face Anti-Spoofing. In: ICASS, IEEE, 2020.

45. Yu Z. et al. Face Anti-Spoofing with Human Material Perception. In: ECCV, 2020.

46. George A., Marcel S. Deep Pixel-Wise Binary Supervision for Face Presentation Attack Detection. In: ICB, 2019, no. CONF.

47. Li X. et al. 3DPC-Net: 3D Point Cloud Network for Face Anti-Spoofing, 2020.

48. Boulkenafet Z. et al. OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations. In: 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), IEEE, 2017, pp. 612-618.

49. Liu Y., Jourabloo A., Liu X. Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision. In: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2018, pp. 389-398.

50. Sulavko A. Biometric-Based Key Generation and User Authentication Using Acoustic Characteristics of the Outer Ear and a Network of Correlation Neurons. In: Sensors, 2022, vol. 22, no. 23, p. 9551.

ПАНФИЛОВА Ирина Евгеньевна, аспирант федерального государственного бюджетного образовательного учреждения высшего образования «Самарский государственный технический университет». 443100, г. Самара, ул. Молодогвардейская, 244. E-mail: panfilova_2015@bk.ru

ЛОЖНИКОВ Павел Сергеевич, проректор по научной и инновационной деятельности федерального государственного автономного образовательного учреждения высшего образования «Омский государственный технический университет». 644050, г. Омск, пр. Мира, 11. E-mail: lozhnikov@gmail.com

PANFILOVA Irina Evgenevna, postgraduate student of the Federal State Budgetary Educational Institution of Higher Education "Samara State Technical University". 443100, Samara, Molodogvardeyskaya str. 244. E-mail: panfilova_2015@bk.ru

LOZHNIKOV Pavel Sergeevich, Vice-Rector for Research and Innovation Activity of the Federal State Autonomous Educational Institution of Higher Education "Omsk State Technical University". 11 Mira Ave., Omsk, 644050, Omsk. E-mail: lozhnikov@gmail.com