

РАЗРАБОТКА АЛГОРИТМА РАСПОЗНАВАНИЯ ЛИЦ НА ОСНОВЕ ГЛУБОКОГО ОБУЧЕНИЯ

Марышева Л.Т., Абдуллаев Д.Б.

*Ташкентский университет информационных технологий имени Мухаммада ал-Хоразмий,
Ташкент, Узбекистан*

*Марышева Л.Т. — доцент кафедры системного и прикладного программирования; Абдуллаев
Д.Б. — магистрант*

Электронная почта: loramarish@mail.ru; dilavar7517@gmail.com

Аннотация. В статье рассматривается разработка алгоритма распознавания лиц на основе глубокого обучения с использованием сверточной сети ResNet-50, функции потерь ArcFace и механизмов внимания. Исходная схема исследования включает детекцию и выравнивание лица, извлечение эмбединга, нормализацию признаков и сопоставление по косинусной близости. Для обучения в исходном материале используется CASIA-WebFace, содержащий 494 414 изображений 10 575 личностей; изображения приводятся к размеру 112×112 пикселей, а предварительная обработка выполняется MTCNN. Методологический анализ показывает, что заявленная высокая точность должна подтверждаться отдельным протоколом тестирования, поскольку приведенный материал содержит параметры модели и распределение обучающей выборки, но не содержит полной таблицы результатов на LFW, порогов принятия решения, ROC-характеристик, FAR/FMR, FRR/FNMR, EER или доверительных интервалов. Поэтому показатель точности выше 99% не трактуется в переработанной версии как независимо подтвержденный экспериментальный результат. Для повышения воспроизводимости уточнены требования к описанию архитектуры внимания, размерности эмбединга, размеру пакета, числу эпох, расписанию скорости обучения, регуляризации, аугментации, аппаратной платформе и случайным начальным условиям. Предложен протокол сравнительной оценки с базовой ResNet-50, ArcFace без внимания и полной моделью, а также внешней проверкой на LFW и более сложных сценариях с окклюзиями, изменением позы и качества изображения. На основе данных NIST выделены дополнительные ограничения, связанные с масками, демографическими различиями и презентационными атаками. Практическое внедрение алгоритма в Узбекистане требует также соблюдения законодательства о биометрических персональных данных, включая требования к согласию, защите и хранению таких данных. Сформулированы направления дальнейшей экспериментальной проверки алгоритма. Особое внимание уделено различию между закрытой классификацией известных классов и открытой биометрической верификацией, где личности тестового набора могут отсутствовать в обучении, а качество определяется ошибками сопоставления при заранее установленном рабочем пороге системы.

Ключевые слова: распознавание лиц, глубокое обучение, CNN, ResNet-50, ArcFace, MTCNN, эмбединг, биометрия, anti-spoofing, верификация.

ВВЕДЕНИЕ

Распознавание лиц относится к наиболее активно развивающимся направлениям компьютерного зрения и применяется в задачах биометрической верификации, контроля доступа, банковской идентификации, видеоаналитики и человеко-машинного взаимодействия. Переход от методов PCA и LDA к

глубоким сверточным нейронным сетям сделал возможным автоматическое формирование устойчивых признаков представлений и существенно улучшил качество распознавания на публичных тестовых наборах [1, 3, 6]. Вместе с тем высокая точность на одном эталонном наборе не гарантирует сопоставимого качества при изменении масштаба галереи, освещения, позы, разрешения, окклюзий и состава пользователей [11, 13–16].

Современная система распознавания лиц является многоэтапной. Как правило, она включает детекцию лица, определение ключевых точек, геометрическое выравнивание, извлечение эмбединга и последующее сопоставление векторов признаков. В исходной работе для предварительной обработки используется MTCNN, а для формирования дескриптора — ResNet-50 в сочетании с ArcFace и механизмами внимания. MTCNN объединяет детекцию лица и локализацию ключевых точек, тогда как ArcFace вводит аддитивный угловой зазор и направлен на повышение межклассовой разделимости признаков [9, 10].

Научная проблема исследования заключается в обеспечении устойчивости биометрического сопоставления в условиях, отличающихся от контролируемого обучающего распределения. Особую сложность представляют частичные перекрытия лица, медицинские маски, большие повороты головы, низкое качество изображений, различия между камерами, демографические вариации и презентационные атаки. Исследования NIST показывают, что результаты существенно зависят от алгоритма и условий эксплуатации, а маски, качество изображения и тип атаки могут заметно изменять частоту ошибок [13–16]. Поэтому корректная оценка модели должна включать не только общую ассигуру, но и рабочие биометрические метрики при фиксированном пороге.

Цель исследования — разработать и методически обосновать алгоритм распознавания лиц на основе ResNet-50, ArcFace и механизмов внимания, а также сформировать воспроизводимый протокол его экспериментальной оценки в условиях открытой биометрической верификации. Для достижения цели необходимо: описать конвейер предварительной обработки и извлечения признаков; формализовать функцию потерь и правило сопоставления; определить структуру обучающих и тестовых данных; установить набор метрик качества; провести сравнительный анализ с базовыми конфигурациями; оценить устойчивость к окклюзиям и качеству изображения; выделить требования к anti-spoofing и практическому развертыванию.

Объектом исследования являются интеллектуальные системы биометрической идентификации по изображению лица. Предмет исследования — алгоритмы извлечения лицевых признаков и сопоставления эмбедингов с использованием глубоких нейронных сетей, угловых функций потерь и механизмов внимания. Рабочая гипотеза заключается в том, что сочетание ArcFace с механизмом внимания может повысить устойчивость признаков к частичным окклюзиям, однако данный эффект должен подтверждаться контролируемым сравнением с моделью без внимания и одинаковым протоколом обучения. Научная новизна переработанной постановки состоит прежде всего в

переходе от декларации высокой ассигуры к воспроизводимой оценке вклада каждого компонента модели по биометрическим метрикам и сценариям ухудшения качества.

ОБЗОР ЛИТЕРАТУРЫ

Исследования глубокого распознавания лиц развивались от прямой классификации идентичностей к обучению метрического пространства. FaceNet предложил оптимизировать компактное эмбединг-пространство с помощью triplet loss, что позволило свести верификацию к сравнению расстояний между векторами [6]. SphereFace и CosFace развили идею углового разделения классов, вводя соответственно multiplicative angular margin и large margin cosine loss [7, 8]. ArcFace предложил аддитивный угловой зазор с прозрачной геометрической интерпретацией на нормированной гиперсфере и показал сильные результаты на нескольких бенчмарках [9]. Эти работы обосновывают выбор угловой функции потерь в исходном исследовании.

Предварительная обработка непосредственно влияет на стабильность дескрипторов. MTCNN объединяет каскадную детекцию лица и оценку ключевых точек, что позволяет нормализовать геометрию изображения перед подачей в сеть [10]. Однако качество входного изображения остается самостоятельным фактором. NIST FATE Part 11 рассматривает автоматическую оценку конкретных дефектов лицевых изображений, что подтверждает необходимость фиксировать размытие, освещение, поворот, экспозицию и другие признаки качества при тестировании системы [16].

Бенчмарк LFW сыграл важную роль в развитии face verification, но его использование как единственного доказательства практической надежности ограничено. MegaFace был создан именно потому, что многие алгоритмы демонстрировали почти идеальные значения на LFW, однако при увеличении галереи до миллиона distractor-изображений качество существенно снижалось [11]. Более поздний WebFace260M также подчеркивает необходимость масштабных обучающих данных и оценки на сложных протоколах, включая IJB-C и сценарии с ограничением времени вывода [12]. Следовательно, показатель «выше 99% на LFW» сам по себе не описывает поведение системы при идентификации в крупной базе или на низкокачественных изображениях.

Окклюзии и медицинские маски являются отдельным источником ошибок. DeepMaskNet ориентирован на распознавание замаскированных лиц [4], а NIST FRVT Part 6B показал, что современные алгоритмы могут адаптироваться к маскам, но уровень ошибок сильно различается между реализациями и зависит от того, закрыто ли лицо на этапе регистрации и проверки [14]. Поэтому утверждение об устойчивости модели к маске должно подтверждаться отдельным тестовым сценарием и соответствующими метриками, а не только визуализацией областей внимания.

Еще одно направление связано с безопасностью биометрии. Обзор Yu и соавторов систематизирует методы face anti-spoofing и показывает важность intra-dataset, cross-dataset, domain-generalization и open-set протоколов [17].

Независимая оценка NIST FATE Part 10, охватившая десятки программных PAD-алгоритмов, выявила значительный разброс результатов по типам презентационных атак; ни один программный метод не оказался универсальным для всех проверенных атак [15]. Это означает, что распознавание личности и проверка «живости» должны рассматриваться как связанные, но разные подсистемы.

Для реального внедрения важна также устойчивость качества между группами пользователей. NISTIR 8280 посвящен демографическим эффектам и показывает необходимость измерять различия в ошибках распознавания на репрезентативных выборках [13]. Следовательно, экспериментальная часть должна включать по возможности анализ качества по полу, возрастным группам и другим доступным атрибутам набора данных, не делая выводов о справедливости модели без прямой проверки.

Таблица 1.

Научные подходы и их значение для алгоритма распознавания лиц

Подход / источник	Ключевая идея	Роль в исследовании
FaceNet [6]	Метрическое обучение эмбедингов и сравнение расстояний.	Формирует базовую логику верификации в признаковом пространстве.
SphereFace / CosFace [7, 8]	Угловые и косинусные margins для повышения разделимости классов.	Показывают эволюцию large-margin функций потерь.
ArcFace [9]	Аддитивный угловой зазор на нормированной гиперсфере.	Основная функция потерь в рассматриваемой модели.
MTCNN [10]	Совместная детекция лица и ключевых точек.	Предварительное выравнивание входных изображений.
MegaFace / WebFace260M [11, 12]	Масштабная оценка и сложные протоколы.	Показывают ограничения одной LFW-accuracy.
NIST FRVT/FATE [13–16]	Независимая оценка демографии, масок, PAD и качества изображений.	Определяет дополнительные сценарии и метрики проверки.

В исходной библиографии представлены обзорные и прикладные работы по глубокому распознаванию, маскам и 1D-CNN [1–5], однако отсутствуют ссылки на ключевые методы, непосредственно использованные в эксперименте: ArcFace, MTCNN, ResNet-подходы и независимые протоколы NIST. Расширение литературной базы устраняет этот разрыв и позволяет отделить реализованные компоненты от методов, которые только рассматриваются как альтернативы.

МЕТОДОЛОГИЯ

Исходный алгоритм рассматривается как последовательность пяти этапов: детекция лица, выравнивание по ключевым точкам, извлечение признаков, нормализация эмбединга и сопоставление по косинусной близости. Для воспроизводимости каждый этап должен быть описан отдельно, поскольку изменение детектора, правила выравнивания, размера входа или порога принятия

решения может изменить итоговые показатели. В исходном материале детектором является MTCNN, размер входа — 112×112 пикселей, backbone — ResNet-50, а функция потерь — ArcFace.

Таблица 2.

Этапы предлагаемого алгоритма

Этап	Операция	Выход
1. Детекция	MTCNN определяет лицо и ключевые точки.	Bounding box и landmarks.
2. Выравнивание	Геометрическая нормализация по landmarks.	Лицо 112×112 RGB.
3. Извлечение признаков	ResNet-50 с механизмом внимания.	Вектор признаков x .
4. Нормализация	L2-нормирование эмбединга.	Нормированный вектор $\hat{x}$.
5. Сопоставление	Косинусная близость и сравнение с порогом τ .	Match / non-match либо ранжированный список.

В исходной работе для обучения указан набор CASIA-WebFace. Сохраняются приведенные авторами статистические характеристики: 494 414 изображений 10 575 личностей, среднее число изображений на класс около 46, RGB-формат и вход 112×112 пикселей. При практической реализации требуется дополнительно документировать способ удаления ошибочных/дублирующихся изображений, политику аугментации и то, разделяются ли личности между обучающей, валидационной и тестовой частями.

Таблица 3.

Статистика набора данных, приведенная в исходной работе

Признак	Значение / количество
Всего изображений	494 414
Количество уникальных личностей	10 575
Среднее количество фото на человека	≈ 46
Размер входного изображения	112×112 px
Формат	RGB
Предварительная обработка	MTCNN: детекция и выравнивание

В исходном документе данные разделены на 445 000 обучающих изображений (90%) и 49 414 контрольных изображений (10%). Такое распределение пригодно для контроля функции потерь, но само по себе не подтверждает open-set качество, если одни и те же идентичности присутствуют одновременно в train и validation. Для биометрической верификации рекомендуется иметь независимый тестовый протокол, например LFW, IJB-C или специально сформированную identity-disjoint выборку, а порог τ выбирать только по валидационной части [7, 11, 18].

Таблица 4.

Разделение данных и требуемое дополнение протокола

Выборка	Количество изображений	Доля	Методическое назначение
Train	445 000	90%	Обучение параметров сети.

Validation	49 414	10%	Выбор гиперпараметров и порога; не заменяет независимый test.
External test	В исходном файле не специфицирован	—	Необходим для подтверждения заявленной точности и обобщающей способности.

Для изображения i сеть формирует эмбединг x_i . После L2-нормализации сходство с весовым вектором класса W_j может выражаться через косинус угла между векторами:

$$\cos(\theta_j) = (x_i \cdot W_j) / (||x_i|| \cdot ||W_j||) \quad (1)$$

ArcFace вводит аддитивный угловой margin m для истинного класса и масштаб s . В компактной форме функция потерь записывается как [9]:

$$L = -(1/N) \sum_i \log [e^{s \cos(\theta_{yi}+m)} / (e^{s \cos(\theta_{yi}+m)} + \sum_{j \neq y_i} e^{s \cos \theta_{ji}})] \quad (2)$$

В исходной работе приведены $m=0,5$, s упоминается в формуле, но его числовое значение не задано. Для полной воспроизводимости необходимо указать s , размерность эмбединга, batch size, число эпох, weight decay, momentum, scheduler, способы аугментации, инициализацию, random seed и критерий остановки. Аналогично требуется описать конкретный тип механизма внимания и места его интеграции в ResNet-50; термин Self-Attention без схемы блока недостаточен для точного повторения эксперимента.

Таблица 5.

Гиперпараметры и пробелы воспроизводимости

Параметр	Значение в источнике	Что требуется уточнить
Backbone	ResNet-50	Версия блока, pretrained/с нуля, размер эмбединга.
Loss	ArcFace	Scale s ; способ нормализации; реализация.
Learning rate	0,001	Scheduler и число эпох.
Optimizer	SGD	Momentum, weight decay.
Margin m	0,5	Проверка чувствительности к m .
Attention	Self-Attention / механизмы внимания	Архитектура блока и точки вставки.
Batch size / seed / hardware	Не указаны	Обязательны для воспроизводимости и оценки вычислительной стоимости.

Для верификации двух лицевых изображений вычисляется косинусная близость $S(x_1, x_2)$. Решение о совпадении принимается при $S \geq \tau$, где τ должен быть определен на независимой валидационной выборке. В отличие от обычной accuracy для закрытой классификации, биометрическое тестирование должно отражать компромисс между ложными совпадениями и ложными отказами. NIST использует показатели false match rate (FMR) и false non-match rate (FNMR); для научной статьи целесообразно также представить ROC, TAR/TPR при фиксированных FAR/FMR, EER и, для 1:N идентификации, Rank-1/Rank-k [13, 14, 18].

$$match(x_1, x_2) = 1, \text{ если } S(x_1, x_2) \geq \tau; \text{ иначе } 0 \quad (3)$$

Чтобы проверить заявленный вклад внимания, эксперимент следует

организовать как ablation study при одинаковых данных и режиме обучения: (A) ResNet-50 с базовой функцией потерь; (B) ResNet-50 + ArcFace; (C) ResNet-50 + ArcFace + attention. Дополнительно целесообразны тесты при искусственных и реальных окклюзиях, ухудшении разрешения, изменении яркости и повороте головы. Такое сравнение позволяет отделить эффект отдельного компонента от эффекта увеличения вычислительной сложности.

АНАЛИЗ И РЕЗУЛЬТАТЫ

На основании исходного материала подтверждается наличие сформированной архитектурной концепции: данные проходят MTCNN-выравнивание, затем обрабатываются ResNet-50, а обучение ориентировано на угловую разделимость классов с использованием ArcFace. Приведены основные гиперпараметры и схема разделения CASIA-WebFace. Эти элементы достаточны для описания общего принципа алгоритма, но недостаточны для независимого воспроизведения конкретного эксперимента без дополнительных настроек, перечисленных в методологии.

Исходная статья заявляет точность выше 99% на эталонных наборах, включая LFW. Однако в представленном файле отсутствуют отдельная таблица результатов LFW, число тестовых пар, способ следования официальному протоколу, выбранный threshold, среднее значение по folds, стандартное отклонение или доверительный интервал. Поэтому в настоящей переработанной версии показатель «выше 99%» рассматривается как утверждение исходного текста, требующее документального подтверждения логам эксперимента или таблицей результатов, а не как заново установленный факт.

Аналогичная проблема относится к заявленному эффекту механизмов внимания. В исходном тексте указано, что карты активации выделяют область глаз, переносицы и контуры лица, однако отсутствует количественное сравнение модели с attention и без него. Визуализация heatmap полезна для интерпретации, но не доказывает повышение качества распознавания. Для подтверждения необходимо показать различия по FMR/FNMR, TAR@FMR, EER или ассигасу на одинаковом тестовом протоколе и оценить статистическую устойчивость результата.

Таблица 6.

Оценка полноты экспериментальных доказательств

Элемент	Что имеется в исходном файле	Статус
CASIA-WebFace	Размер и число классов; 90/10 split.	Описано, но нет identity-disjoint test.
ResNet-50 + ArcFace	Backbone, loss, LR, SGD, m=0,5.	Частично воспроизводимо; отсутствуют важные параметры.
Attention	Упоминается Self-Attention и heatmaps.	Нужны схема и ablation study.
LFW >99%	Текстовое утверждение.	Не подтверждено таблицей собственного эксперимента.
Маски / окклюзии	Качественное описание устойчивости.	Нужны отдельные тестовые сценарии.

Anti-spoofing	Указано как направление дальнейшей работы.	Не является реализованной частью текущей модели.
---------------	--	--

Сопоставление с независимыми источниками показывает, почему расширение протокола принципиально. MegaFace демонстрирует, что высокое качество на LFW может заметно ухудшаться при масштабировании базы [11]. NIST показывает, что маски могут увеличивать частоту ошибок и что результаты сильно различаются между алгоритмами [14], а оценка PAD выявляет зависимость эффективности от конкретного вида презентационной атаки [15]. Следовательно, практическая надежность алгоритма должна характеризоваться набором сценариев, а не одним итоговым процентом.

Для будущей экспериментальной версии статьи рекомендуется сохранить исходную архитектуру как гипотезу и дополнить ее воспроизводимым журналом эксперимента. Минимальный набор результатов должен включать: LFW verification по официальному протоколу; ROC и EER; TAR при нескольких FMR; ablation study; оценку на окклюзиях/масках; скорость вывода и размер модели; при наличии данных — subgroup-анализ. Только после этого можно количественно утверждать, что внимание улучшает ArcFace-базу и что модель пригодна для заявленных практических сценариев.

ОБСУЖДЕНИЕ

Первое ограничение связано с различием между задачей классификации обучающих идентичностей и открытой биометрической верификацией. Если train и validation содержат одних и тех же людей, высокое качество на validation может отражать способность различать известные классы, но не обязательно способность обобщаться на новые личности. SphereFace и другие методы large-margin face recognition прямо ориентированы на open-set постановку [7]. Поэтому тестирование должно проводиться на идентичностях, которые не использовались для оптимизации весов и порога.

Второе ограничение — недостаточность метрики accuracy. В прикладной биометрии стоимость ложного совпадения и ложного отказа различается в зависимости от сценария: банковская аутентификация, контроль доступа или поиск по большой галерее предъявляют разные требования к FMR/FNMR. NIST оценивает алгоритмы при конкретных рабочих точках, а также отдельно рассматривает 1:1 и 1:N режимы [13, 14, 18]. Поэтому рабочий порог должен определяться до тестирования, а результаты должны сопровождаться ROC или DET-кривой и значениями ошибок при заданных порогах.

Третье ограничение — отсутствие количественного доказательства преимуществ attention-модуля. Механизм внимания теоретически может перераспределять вес с закрытых областей на доступные части лица, но это не означает автоматического улучшения в каждом датасете. Необходима ablation-схема, где все остальные параметры фиксированы. Если улучшение наблюдается только на обучающем распределении или исчезает на внешнем наборе, это может указывать на переобучение.

Четвертое ограничение связано с масками, качеством и масштабом. NIST

показывает, что даже между современными алгоритмами сохраняется существенный разброс качества на замаскированных лицах [14]. FATE Part 11 выделяет дефекты изображения как самостоятельный объект оценки [16], а MegaFace показывает, что результат на небольшой benchmark-галерее не всегда переносится на миллионный масштаб [11]. Это требует сценарного тестирования по нескольким уровням качества и размеру галереи.

Пятое ограничение — отсутствие самостоятельного модуля защиты от presentation attacks. Текущий алгоритм решает задачу распознавания, но не подтверждает, что вход получен от живого человека. По данным NIST FATE Part 10 результаты программного PAD значительно различаются между типами атак, а универсального решения для всех проверенных атак не выявлено [15]. Следовательно, для банковской или дистанционной идентификации следует отдельно проектировать PAD/anti-spoofing и оценивать его по специализированным метрикам [17].

Шестое ограничение — отсутствие анализа демографической устойчивости. NISTIR 8280 показывает, что ошибки распознавания могут различаться между демографическими группами и между алгоритмами [13]. В исходной статье такой анализ отсутствует. Это не позволяет делать вывод о равномерности качества модели для разных групп пользователей; для подобного вывода нужна репрезентативная тестовая выборка и отчет по группам.

Седьмое ограничение связано с правовыми условиями практического применения в Узбекистане. Закон Республики Узбекистан «О персональных данных» относит сведения об анатомических и физиологических особенностях, используемые для идентификации, к биометрическим данным. Их обработка для установления личности в общем случае требует согласия субъекта, за исключением предусмотренных законом случаев; действующая редакция также предусматривает обязательное хранение биометрических данных физических лиц на территории Республики Узбекистан [19, 20]. Поэтому архитектура промышленной системы должна включать правовое основание обработки, контроль доступа, защиту шаблонов и локализацию хранения данных.

С учетом выявленных ограничений практическая ценность исследования заключается не в одном заявленном проценте точности, а в формировании проверяемого конвейера: качественная предобработка, дискриминативные эмбединги ArcFace, механизм внимания как проверяемая гипотеза, независимое тестирование, управление порогом и отдельный контур anti-spoofing. Такая структура позволяет превратить экспериментальную модель в систему, качество которой можно объективно сопоставлять с альтернативами.

ЗАКЛЮЧЕНИЕ

В работе систематизирован алгоритм распознавания лиц на основе ResNet-50, ArcFace и механизмов внимания. Сохранены исходные характеристики CASIA-WebFace, схема MTCNN-предобработки и основные гиперпараметры. Методологически уточнено, что задача распознавания должна рассматриваться как открытая биометрическая верификация или идентификация, где ключевым

объектом является качество эмбединга и поведение системы при фиксированном рабочем пороге.

Проведенный анализ выявил существенный разрыв между архитектурным описанием и доказательной частью исходной статьи. Заявление о точности выше 99% не сопровождается полной таблицей LFW-эксперимента, а преимущества attention-модуля не подтверждены ablation-сравнением. Отсутствуют также FMR/FNMR, EER, ROC, доверительные интервалы, внешний test-протокол, часть гиперпараметров и вычислительные характеристики. Поэтому эти элементы определены как обязательные направления доработки, а не заменены искусственно созданными числовыми результатами.

Расширенный обзор источников показывает, что надежность face recognition должна проверяться при масштабировании галереи, масках, дефектах изображения, демографических вариациях и презентационных атаках. ArcFace имеет обоснованную роль как функция обучения дискриминативных признаков, однако реальная устойчивость конкретной реализации определяется данными, протоколом тестирования и архитектурными деталями. Для промышленного применения распознавание должно дополняться отдельным PAD-модулем и контролем качества входных данных.

Дальнейшее исследование целесообразно направить на воспроизводимое обучение трех сопоставимых конфигураций — базовой ResNet-50, ResNet-50 + ArcFace и ResNet-50 + ArcFace + attention — с внешним тестированием на LFW и более сложном наборе, например IJB-C, а также на сценариях окклюзии и снижения качества. Дополнительно требуется оценить скорость вывода, объем памяти, устойчивость порога и требования законодательства Узбекистана к обработке биометрических персональных данных.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Guo G., Zhang N. A survey on deep learning based face recognition // Computer Vision and Image Understanding. 2019. Vol. 189. Art. 102805. DOI: 10.1016/j.cviu.2019.102805.
2. Dubey R.K., Choubey D.K. Deconstructive human face recognition using deep neural network // Multimedia Tools and Applications. 2023. Vol. 82, No. 22. P. 34147–34162. DOI: 10.1007/s11042-023-15107-4.
3. Wickrama Arachchilage S.P.K., Izquierdo E. Deep-learned faces: a survey // EURASIP Journal on Image and Video Processing. 2020. Art. 25. DOI: 10.1186/s13640-020-00510-w.
4. Ullah N. et al. A novel DeepMaskNet model for face mask detection and masked facial recognition // Journal of King Saud University - Computer and Information Sciences. 2022. Vol. 34, No. 10. P. 9905–9914. DOI: 10.1016/j.jksuci.2021.12.017.
5. Mohammed Sahan J., Abbas E.I., Abood Z.M. A facial recognition using a combination of a novel one dimension deep CNN and LDA // Materials Today: Proceedings. 2023. Vol. 80. P. 3594–3599. DOI: 10.1016/j.matpr.2021.07.325.
6. Schroff F., Kalenichenko D., Philbin J. FaceNet: A Unified Embedding for Face Recognition and Clustering // Proceedings of CVPR. 2015. P. 815–823. DOI:

10.1109/CVPR.2015.7298682.

7. Liu W., Wen Y., Yu Z., Li M., Raj B., Song L. SphereFace: Deep Hypersphere Embedding for Face Recognition // Proceedings of CVPR. 2017. P. 212–220. URL: https://openaccess.thecvf.com/content_cvpr_2017/html/Liu_SphereFace_Deep_Hypersphere_CVPR_2017_paper.html.

8. Wang H., Wang Y., Zhou Z. et al. CosFace: Large Margin Cosine Loss for Deep Face Recognition // Proceedings of CVPR. 2018. P. 5265–5274. URL: https://openaccess.thecvf.com/content_cvpr_2018/html/Wang_CosFace_Large_Margin_CVPR_2018_paper.html.

9. Deng J., Guo J., Xue N., Zafeiriou S. ArcFace: Additive Angular Margin Loss for Deep Face Recognition // Proceedings of CVPR. 2019. P. 4690–4699. URL: https://openaccess.thecvf.com/content_CVPR_2019/html/Deng_ArcFace_Additive_Angular_Margin_Loss_for_Deep_Face_Recognition_CVPR_2019_paper.html.

10. Zhang K., Zhang Z., Li Z., Qiao Y. Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks // IEEE Signal Processing Letters. 2016. Vol. 23, No. 10. P. 1499–1503. DOI: 10.1109/LSP.2016.2603342.

11. Kemelmacher-Shlizerman I., Seitz S.M., Miller D., Brossard E. The MegaFace Benchmark: 1 Million Faces for Recognition at Scale // Proceedings of CVPR. 2016. P. 4873–4882. URL:

https://openaccess.thecvf.com/content_cvpr_2016/html/Kemelmacher-Shlizerman_The_MegaFace_Benchmark_CVPR_2016_paper.html.

12. Zhu Z., Huang G., Deng J. et al. WebFace260M: A Benchmark Unveiling the Power of Million-Scale Deep Face Recognition // Proceedings of CVPR. 2021. P. 10492–10502. URL:

https://openaccess.thecvf.com/content/CVPR2021/html/Zhu_WebFace260M_A_Benchmark_Unveiling_the_Power_of_Million-Scale_Deep_Face_CVPR_2021_paper.html.

13. Grother P., Ngan M., Hanaoka K. Face Recognition Vendor Test Part 3: Demographic Effects. NISTIR 8280. 2019. DOI: 10.6028/NIST.IR.8280.

14. Ngan M.L., Grother P.J., Hanaoka K.K. Ongoing Face Recognition Vendor Test Part 6B: Face Recognition Accuracy with Face Masks Using Post-COVID-19 Algorithms. NISTIR 8331. 2020. DOI: 10.6028/NIST.IR.8331.

15. Ngan M.L., Grother P.J., Hom A. Face Analysis Technology Evaluation Part 10: Performance of Passive, Software-based Presentation Attack Detection Algorithms. NISTIR 8491. 2023. DOI: 10.6028/NIST.IR.8491.

16. Yang J., Grother P.J., Ngan M.L., Hanaoka K.K., Hom A. Face Analysis Technology Evaluation Part 11: Face Image Quality Vector Assessment: Specific Image Defect Detection. NISTIR 8485. 2023. DOI: 10.6028/NIST.IR.8485.

17. Yu Z., Qin Y., Li X., Zhao C., Lei Z., Zhao G. Deep Learning for Face Anti-Spoofing: A Survey // IEEE Transactions on Pattern Analysis and Machine Intelligence. 2023. Vol. 45, No. 5. P. 5609–5631. DOI: 10.1109/TPAMI.2022.3215850.

18. National Institute of Standards and Technology. Face Challenges: IARPA Janus Benchmark-C (IJB-C), FRVT/FRTE evaluation resources. Updated 2025. URL: <https://www.nist.gov/programs-projects/face-challenges>.

19. Закон Республики Узбекистан от 02.07.2019 № ЗРУ-547 «О персональных данных», ст. 26–27¹ (действующая редакция). Национальная база данных законодательства Республики Узбекистан. URL: <https://lex.uz/docs/4396419>.

20. Закон Республики Узбекистан от 26.03.2026 № ЗРУ-1125 «О внесении изменений и дополнения в Закон Республики Узбекистан “О персональных данных”». Национальная база данных законодательства Республики Узбекистан. URL: <https://lex.uz/docs/8104580>.