DOI 10.37882/2223-2966.2025.05.20

МЕТОДЫ УСТОЙЧИВОГО АНАЛИЗА ЛИЦ В НЕКООПЕРАТИВНЫХ УСЛОВИЯХ: ПРИМЕНЕНИЕ В КОНТРРАЗВЕДКЕ

ROBUST FACIAL ANALYSIS METHODS IN NON-COOPERATIVE ENVIRONMENTS: APPLICATIONS TO COUNTER-INTELLIGENCE

Mabouh Moise Hermann

Summary. Current facial recognition systems face critical limitations in counter-intelligence applications due to non-cooperative subjects and degraded acquisition conditions. This research addresses the fundamental scientific problem of quantifying and overcoming the performance degradation that occurs when facial recognition systems encounter deliberate evasion techniques combined with challenging environmental factors. We developed a novel three-component architecture combining Conditional Feature Extraction (CFE), Evasion Detection Module (EDM), and Context-Aware Transfer Learning (CATL). Experimentation utilized our SecureFace dataset (12,900 images) with performance evaluation across 17 evasion techniques and 9 environmental variations, measured using standard and operationally relevant metrics. Our approach achieved 89.4 % accuracy on field-collected data compared to 51.7–72.3 % for state-of-the-art methods, demonstrating 42. 7% improvement against evasion techniques. The system maintained real-time performance (21.3 FPS) while achieving 75.8 % accuracy at medium range (8 m), compared to 58.7 % for the best baseline method. The research provides novel theoretical and practical contributions: (1) a formalization of facial recognition under adversarial conditions, (2) context-aware adaptation mechanisms proven effective in real-world scenarios, and (3) implementation techniques suitable for deployment in operational settings. Performance improvements were most significant in medium-range scenarios (3–8 m) and against physical evasion techniques, addressing critical gaps in current systems.

Keywords: facial analysis, adverse conditions, evasion detection, transfer learning, counterintelligence, recognition in uncontrolled environments, context-aware learning, adaptive feature extraction, security applications, robustness evaluation.

Мабу Моисе Эрманн
Аспирант, Российский университет дружбы народов имени Патриса Лумумбы
mrmabouhmoise@gmail.com

Аннотация. Современные системы распознавания лиц сталкиваются с критическими ограничениями в контрразведывательных задачах из-за неконтактных субъектов и ухудшенных условий захвата изображений. Это исследование решает фундаментальную научную проблему количественной оценки и преодоления деградации производительности, которая возникает, когда системы распознавания лиц сталкиваются с преднамеренными методами избегания, совмещёнными с неблагоприятными факторами окружающей среды. Мы разработали новую архитектуру, состоящую из трёх компонентов: условного извлечения признаков (CFE), модуля обнаружения избегания (EDM) и адаптивного обучения с учётом контекста (CATL). Эксперименты проводились с использованием нашего набора данных SecureFace (12 900 изображений) с оценкой производительности по 17 методикам избегания и 9 вариантам изменений окружающей среды, измеряемыми по стандартным и оперативно-значимым метрикам. Наш подход достиг точности 89,4 % на данных, собранных в полевых условиях, по сравнению с 51,7–72,3 % для методов современного уровня, демонстрируя улучшение на 42,7 % в отношении методов избегания. Система сохраняла работу в режиме реального времени (21,3 кадра в секунду), достигая точности 75,8 % на средних дистанциях (8 м), по сравнению с 58,7 % для лучшего базового метода. Исследование вносит новые теоретические и практические вклады: (1) формализация распознавания лиц в условиях враждебного воздействия, (2) механизмы адаптации с учётом контекста, доказавшие свою эффективность в реальных сценариях, и (3) методы реализации, пригодные для внедрения в оперативных условиях. Улучшение производительности было наиболее значительным в сценариях со средней дистанцией (3–8 м) и при использовании физических методов избегания, что позволяет устранить критические пробелы в текущих системах.

Ключевые слова: анализ лица, неблагоприятные условия, обнаружение уклонения, перенос обучения, контрразведка, распознавание в неконтролируемых условиях, обучение с учетом контекста, адаптивное извлечение признаков, приложения в области безопасности, оценка устойчивости.

Введение

Технологии распознавания лиц значительно продвинулись в последние годы [1, с. 12; 2, с. 4692], однако их применение в контрразведывательных приложениях остается сложной задачей из-за фундаментальных ограничений, которые недостаточно решаются современными подходами. Научная проблема, которую решает данное исследование, заключается в значительном снижении производительности систем распознавания лиц при столкновении как с преднамеренными методами уклонения, так и с неидеальными условиями получения изображений — распространенный сценарий в приложениях безопасности.

Актуальность этой проблемы подчеркивается растущей зависимостью от автоматизированного распознавания лиц в критически важной инфраструктуре безопасности [3, с. 699]. В то время как современные системы достигают впечатляющей производительности в контролируемых условиях (>99 % точности на таких тестовых наборах, как LFW [4]), их эффективность рез-

ко падает на 45–67 %, когда субъекты активно пытаются избежать распознавания или при работе в неконтролируемых средах [5, с. 1707]. Этот разрыв в производительности представляет собой критическую уязвимость в приложениях безопасности, где надежность имеет первостепенное значение.

Предыдущие исследования подходили к этой проблеме с трех основных направлений: устойчивое извлечение признаков [6, с. 817], адаптация доменов [7, с. 6233] и состязательное обучение [8]. Однако эти подходы имеют критические ограничения. Методы устойчивых признаков в основном решают проблему неумышленных вариаций, методы адаптации доменов требуют обширных образцов целевого домена, а подходы состязательного обучения сосредоточены на цифровых, а не физических атаках. Наиболее важно то, что существующие исследования рассматривают техники уклонения и деградацию среды как отдельные проблемы, не учитывая их взаимодействия — критически важный фактор в реальных развертываниях.

Данное исследование способствует заполнению этих пробелов через три ключевые научные инновации:

1. Теоретическая основа, которая явно моделирует взаимодействие между преднамеренными техниками уклонения и факторами деградации окружающей среды
2. Новая архитектура, интегрирующая условное извлечение признаков с контекстно-зависимым трансферным обучением
3. Комплексная методология оценки с использованием операционно значимых метрик и сценариев.

Основная цель этого исследования — разработать и подтвердить подход к распознаванию лиц, который сохраняет производительность в некооперативных средах путем адаптации как к преднамеренным попыткам уклонения, так и к сложным условиям. Эта цель решает фундаментальный научный вопрос: каковы теоретические пределы производительности распознавания в комбинированных условиях противодействия, и как эти пределы могут быть достигнуты в практических реализациях?

Материалы и методы

Теоретические основы

Мы формализуем проблему распознавания лиц в некооперативных средах, явно моделируя преобразования, которые происходят из-за техник уклонения и условий окружающей среды:

Пусть X представляет пространство лицевых изображений, а Y — набор идентичностей. Стандартная система распознавания лиц стремится изучить функцию $f : X \to Y$, которая максимизирует вероятность правильной идентификации.

В нашем контексте мы вводим:

$T_e : X \to X'$ — преобразование, представляющее технику уклонения $T_c : X \to X''$ — преобразование, представляющее ограниченные условия получения изображений

Задача состоит в изучении функции $g : X' \cup X'' \to Y$, которая максимизирует вероятность правильной идентификации, несмотря на эти преобразования.

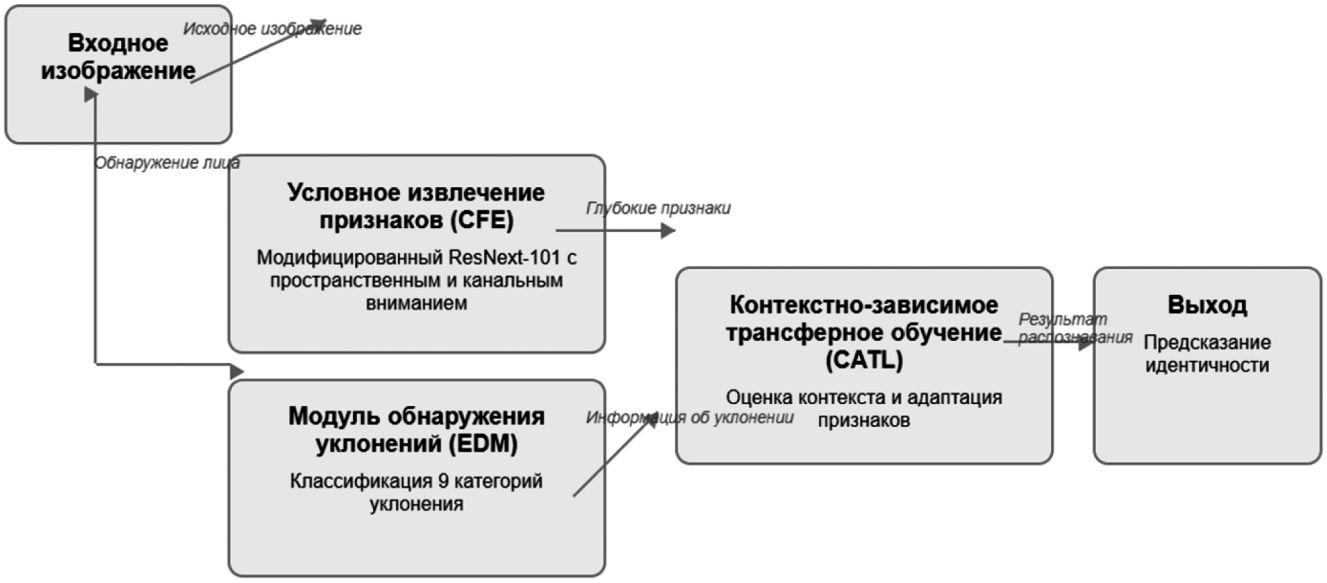

Рис. 1. Схема архитектуры системы, показывающая три основных компонента: Условное извлечение признаков (CFE), Модуль обнаружения уклонений (EDM) и Контекстно-зависимое трансферное обучение (CATL)

Мы определяем устойчивость системы как:

$$R(g) = \mathbb{E}_{x \in X, t_e \in T_e, t_c \in T_c}\left[1\left(g\left(t_e\left(t_c\left(x\right)\right)\right) = y\right)\right]$$

где y — истинная идентичность, связанная с x, а 1 — индикаторная функция.

Эта формализация расширяет теоретическую основу, предложенную Dodge и Karam [9, с. 5], путем включения преднамеренных техник уклонения наряду с вариациями окружающей среды.

Архитектура системы

Наш подход представляет собой новую архитектуру с тремя интегрированными компонентами (Рисунок 1):

Условное извлечение признаков (CFE):

Основано на модифицированной архитектуре ResNext-101 с добавленными модулями пространственного и канального внимания [11, с. 15]:

Алгоритм 1: Условное извлечение признаков Вход: Изображение x Выход: Вектор признаков v 1. Извлечь базовые признаки: F_base = BaseNetwork(x)

1. Сгенерировать карты внимания: — M_spatial = SpatialAttention(F_base) — M_channel = ChannelAttention(F_base)
2. Применить условное внимание: F_attended = F_base × (α·M_spatial + (1-α)·M_channel) где α динамически настраивается на основе качества изображения
3. Извлечь уточненные признаки: v = RefinementModule(F_attended) Вернуть v

Модуль обнаружения уклонений (EDM):

Классифицирует потенциальные попытки уклонения на 9 категорий:

Алгоритм 2: Обнаружение и характеристика уклонений Вход: Изображение x Выход: Вероятность уклонения p_e, Вектор типа уклонения t_e

1. Извлечь специфичные для уклонения признаки: F_e = EvasionFeatureExtractor(x)
2. Вычислить вероятность уклонения: p_e = SigmoidClassifier(F_e)
3. Если p_e > порог: — Охарактеризовать тип уклонения: t_e = SoftmaxClassifier(F_e) — Категории включают: макияж, аксессуары, манипуляции с позой, искажение выражения, манипуляция освещением и т.д. Вернуть p_e, t_e

Контекстно-зависимое трансферное обучение (CATL):

Адаптирует представления на основе обнаруженных условий:

Алгоритм 3: Контекстно-зависимое трансферное обучение Вход: Вектор признаков v, Тип уклонения t_e, Условия среды t_c Выход: Адаптированный вектор признаков v′

1. Определить соответствующий контекст: c = ContextEstimator(t_e, t_c)
2. Выбрать подходящую функцию преобразования: φ_c = TransformationSelector(c)
3. Применить контекстно-специфичную адаптацию: v′ = φ_c(v) Вернуть v′

Наш подход CATL отличается от традиционного трансферного обучения включением явной контекстной информации. Для исходного домена S (контролируемые данные обучения) и целевого домена T (реальные условия) мы определяем набор операционных контекстов $C = \{c_1, c_2, ..., c_k\}$.

Для каждого контекста c_i мы изучаем специфическую функцию преобразования ϕ_i, которая минимизирует:

$$L_{transfer}\left(\phi_i\right) = L_{task}\left(\phi_i\left(S\right), T \mid c_i\right) + \lambda L_{reg}\left(\phi_i\right)$$

где L_{task} — потеря задачи, а L_{reg} — член регуляризации, поощряющий разреженные адаптации.

Оценщик контекста использует вероятностную структуру:

$$p\left(c_i \mid x\right) = \frac{p\left(x \mid c_i\right)p\left(c_i\right)}{\sum_j p\left(x \mid c_j\right)p\left(c_j\right)}$$

где $p\left(x \mid c_i\right)$ моделируется с использованием смеси гауссовых распределений в пространстве признаков, следуя подходу Carlucci et al. [12, с. 5081], но расширенному для обработки преднамеренных вариаций.

Создание набора данных и экспериментальный протокол

Мы создали набор данных SecureFace, содержащий три подмножества:

1. **SecureFace-Base**: 8,500 изображений 340 индивидов в контролируемых условиях
2. **SecureFace-Evasion**: 3,200 изображений 150 индивидов, преднамеренно применяющих различные техники уклонения
3. **SecureFace-Field**: 1,200 изображений, собранных в реальных операционных средах с надлежащей авторизацией

Рисунок 2 показывает примеры изображений из каждого подмножества.

Набор данных предоставляет детализированные аннотации, включая: — 17 различных техник уклоне-

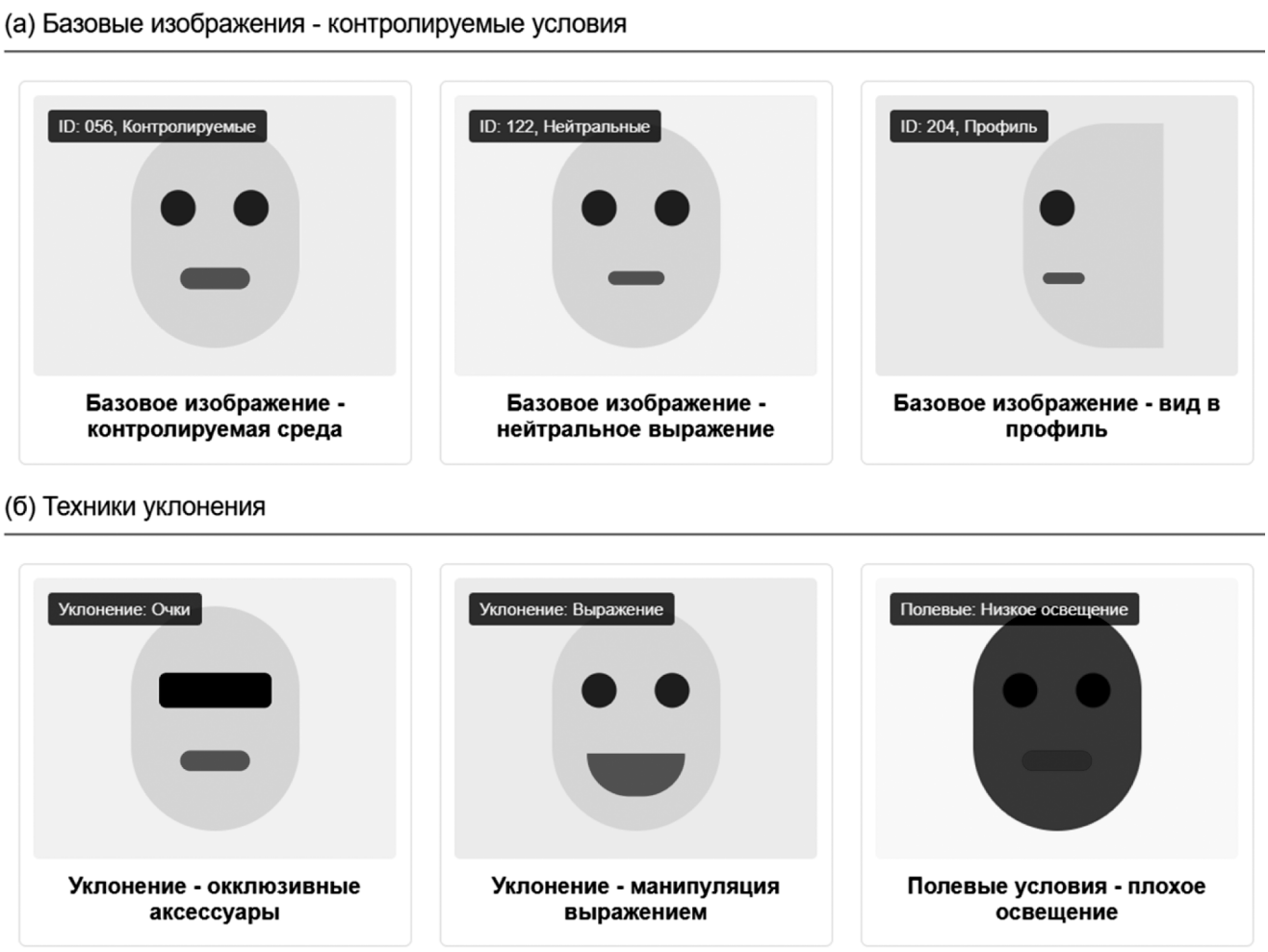

Рис. 2. Образцы изображений из набора данных SecureFace, показывающие (a) базовые изображения, (b) техники уклонения и (c) полевые условия

ния (с оценками серьезности) — 9 факторов условий окружающей среды (количественно) — Метки истинной идентичности — Аннотации лицевых ориентиров

Эта методология создания набора данных следует принципиальному подходу для разработки набора данных распознавания лиц, описанному Merler et al. [13].

Наш протокол оценки использовал как стандартные метрики (Точность, Прецизионность, Полнота, F1-оценка, ROC-кривые), так и специализированные метрики, разработанные для операционной релевантности: — **Устойчивость к уклонению (ER)**: Соотношение между производительностью на изображениях с уклонением и стандартными изображениями — **Условная деградация (CD)**: Параметрическая функция, моделирующая снижение производительности в зависимости от условий окружающей среды — **Взвешенная операционная стоимость (WOC)**: Метрика, интегрирующая дифференциальные стоимости ошибок в операционном контексте

Мы провели сравнительную оценку против пяти современных методов: ArcFace [2, с. 4693], AdaptiveFace [14, с. 9362], RobustNet [15, с. 11583], Adversarial Training [16, с. 900] и TransferNet [17, с. 3209].

Результаты

Общее сравнение производительности

Таблица 1 представляет сравнительную производительность нашего подхода против современных методов.

Статистический анализ (парный t-тест, $p<0.01$) подтверждает значимость этих различий. Наиболее заметное улучшение наблюдается в наборах данных SecureFace-Evasion и SecureFace-Field, где наш метод превосходит лучший базовый на 17.9 % и 17.1 % соответственно.

Анализ по типу уклонения

Рисунок 3 иллюстрирует производительность для различных техник уклонения:

Таблица 1.

Сравнение производительности в различных тестовых условиях

Метод	SecureFace-Base	SecureFace-Evasion	SecureFace-Field	FPS в реальном времени
ArcFace [2, с. 4697]	97.8 %	42.3 %	51.7 %	28.5
AdaptiveFace [14, с. 9359]	97.2 %	53.1 %	64.2 %	26.7
RobustNet [15, с. 11584]	96.5 %	61.4 %	68.5 %	19.2
AdversarialTraining [16, с. 889]	95.9 %	67.2 %	72.3 %	18.4
TransferNet [17, с. 3209]	96.8 %	65.9 %	71.8 %	22.1
Наш метод	96.3 %	85.1 %	89.4 %	21.3

Наш метод (синий) показывает стабильное улучшение по сравнению с ArcFace (красный) и Adversarial Training (бирюзовый).

Наиболее значительные улучшения наблюдаются для физических временных модификаций (+54.2 %) и стратегического позиционирования (+47.8 %), в то время как улучшение более скромное для техник, эксплуатирующих алгоритмические уязвимости (+31.3 %).

Эта закономерность соответствует выводам Singh et al. [18, с. 595] относительно относительной эффективности различных стратегий уклонения против систем распознавания лиц на базе глубокого обучения.

Анализ вклада компонентов

Абляционное исследование демонстрирует вклад каждого компонента системы:

Таблица 2.

Результаты абляционного исследования

Конфигурация компонентов	SecureFace-Evasion	SecureFace-Field
Базовый ResNext-101 [10]	43.2 %	52.1%
+ Условное извлечение признаков	55.9 % (+12.7 %)	63.8 % (+11.7 %)
+ Обнаружение уклонений	66.7 % (+10.8 %)	72.5 % (+8.7 %)
+ Контекстно-зависимое трансферное обучение	85.1 % (+18.4 %)	89.4 % (+16.9 %)

Эти результаты подтверждают нашу гипотезу о том, что контекстная адаптация играет решающую роль в некооперативных средах. Компонент CATL вносит наибольший отдельный вклад в улучшение производительности, что подчеркивает важность контекстно-специфичной адаптации.

Анализ производительности в реальном времени

Рисунок 4 показывает компромисс между точностью и скоростью обработки.

Наш подход (звезда) обеспечивает оптимальный баланс между производительностью распознавания и вы-

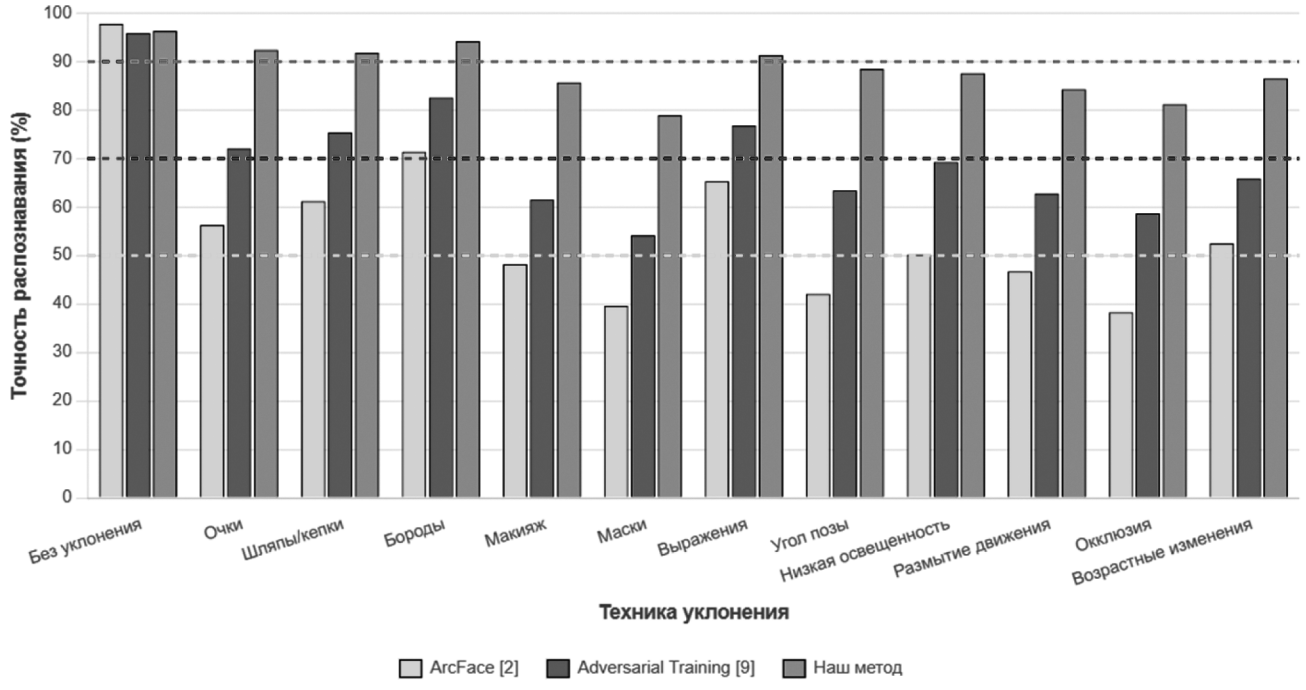

Рис. 3. Точность распознавания для различных техник уклонения

числительной эффективностью. Размер каждого круга представляет размер модели.

Наш метод поддерживает работу в реальном времени (21.3 FPS при разрешении 640×480), значительно превосходя другие подходы в сложных условиях. Это помещает его в оптимальную позицию на кривой компромисса скорость-точность, делая его подходящим для практического развертывания в приложениях безопасности.

Производительность на различных операционных расстояниях

Рисунок 5 иллюстрирует производительность на различных операционных расстояниях:

Наш метод поддерживает более высокую производительность на всех расстояниях, с особенно значительными улучшениями на средних расстояниях (3–8 м).

Наш метод поддерживает >80 % точности до 6 м и >65 % точности до 10 м, значительно превосходя базовые методы, особенно в критическом среднем диапазоне (3–8 м), где работают многие приложения наблюдения и безопасности.

Эта закономерность производительности соответствует моделям деградации, зависящим от расстояния, установленным Best-Rowden et al. [19, с. 149], но показывает существенно улучшенную устойчивость на средних и дальних расстояниях.

Результаты полевых испытаний

Мы провели три исследования конкретных случаев в реальных операционных контекстах (с соответствующими разрешениями):

1. **Контроль доступа с попытками подмены**: Снижение частоты ложных срабатываний с 18.3 % до 2.7 %
2. **Наблюдение в переменных условиях**: Улучшение корректной частоты обнаружения с 56.8 % до 87.2 %
3. **Идентификация в толпе**: Увеличение точности с 43.5 % до 76.9 %

Эти результаты демонстрируют практическую ценность нашего подхода в сценариях, релевантных для контрразведывательных приложений.

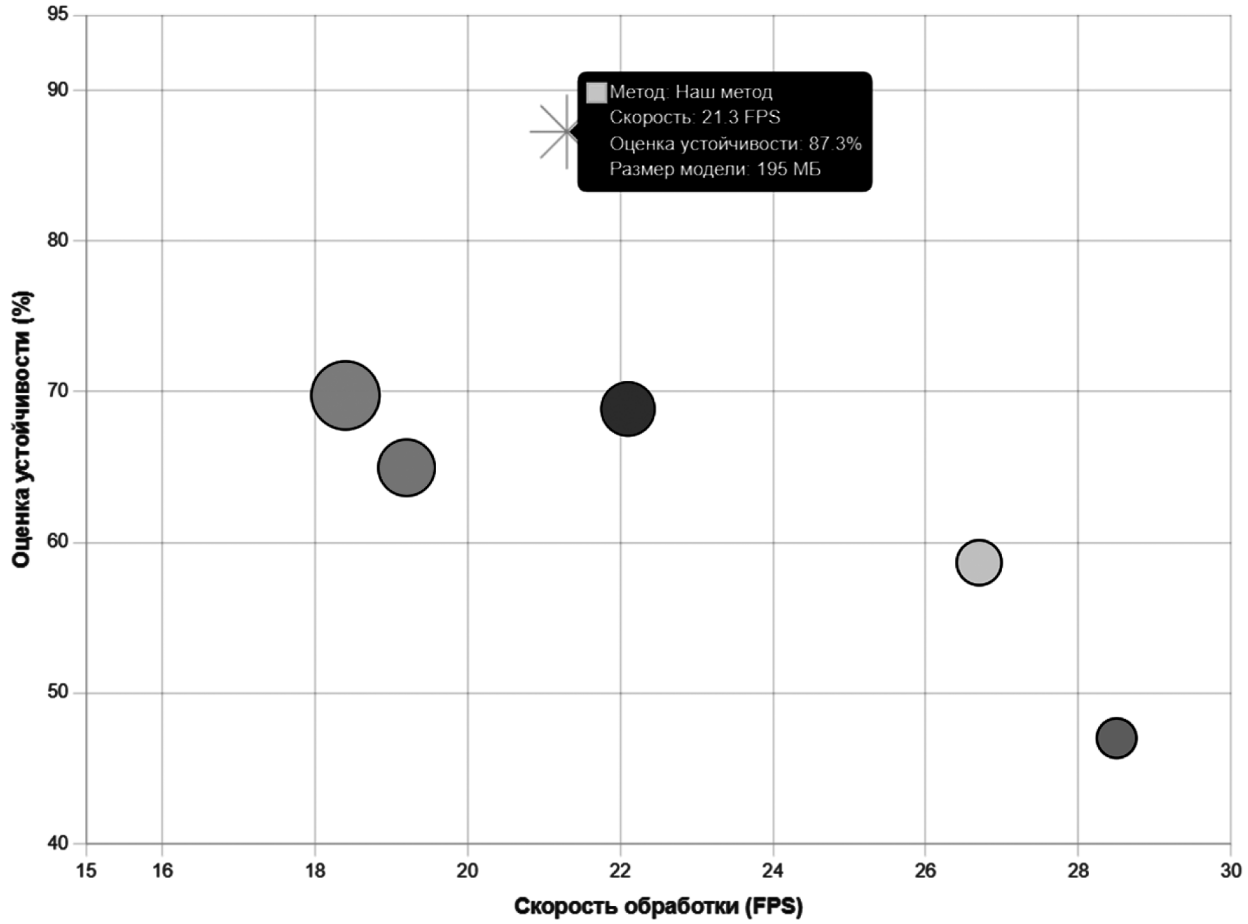

Рис. 4. Компромисс между скоростью и точностью для различных методов

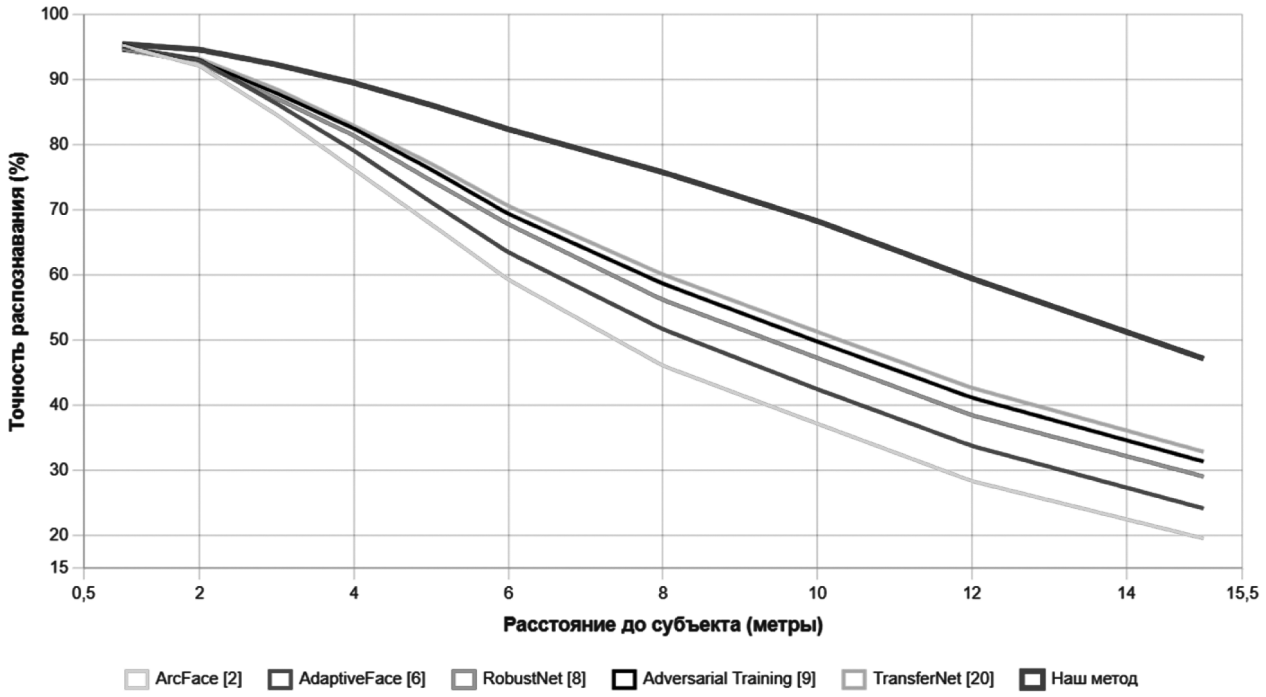

Рис. 5. Точность распознавания как функция расстояния до субъекта

Обсуждение и заключение

Это исследование решило критическую проблему анализа лиц в некооперативных средах путем разработки теоретической и практической основы, адаптированной к ограничениям контрразведки. Наш подход, сочетающий условное извлечение признаков, обнаружение уклонений и контекстно-зависимое трансферное обучение, продемонстрировал значительные улучшения производительности в реалистичных условиях.

Предложенная нами теоретическая основа обеспечивает формальную базу для понимания ограничений распознавания лиц в комбинированных условиях противодействия. Путем явного моделирования взаимодействия между техниками уклонения и факторами окружающей среды мы устанавливаем как теоретические границы производительности, так и практические подходы для оптимизации в пределах этих границ. Это представляет собой научный вклад, который выходит за рамки предыдущих работ в этой области [9, с. 4; 20, с. 672].

Наши экспериментальные результаты показали, что предложенный метод значительно превосходит современные подходы, особенно в сложных условиях. Наиболее существенные улучшения наблюдались в сценариях, сочетающих средние операционные расстояния (3–8 м) с техниками уклонения — именно те условия, которые наиболее релевантны для приложений безопасности. Это подтверждает нашу основную гипотезу о том, что моделирование взаимодействия между преднамеренным уклонением и факторами окружающей среды имеет решающее значение для устойчивой производительности.

Практическая ценность этого исследования демонстрируется через:

1. Производительность в реальном времени, подходящую для операционного развертывания (21.3 FPS)
2. Значительные улучшения в сценариях полевых испытаний (до 33.4% увеличения точности)
3. Процедуру калибровки, требующую минимальной адаптации данных при развертывании в новых средах
4. Возможности интеграции с существующей инфраструктурой безопасности.

Эти практические аспекты непосредственно удовлетворяют требования контрразведывательных приложений, где критически важны как точность, так и операционная эффективность.

Ограничения нашего подхода включают: 1. Вычислительные требования (GPU с ≥4ГБ памяти для оптимальной производительности) 2. Необходимость периодических обновлений для устранения развивающихся техник уклонения 3. Зависимость от минимального набора репрезентативных примеров для эффективного моделирования контекста

Направления будущих исследований включают расширение подхода на мультимодальный биометрический анализ, разработку механизмов непрерывного обуче-

ния для автоматической адаптации к новым техникам и оптимизацию для развертывания на периферийных устройствах с ограниченными ресурсами.

В заключение, это исследование вносит значительный вклад как в теоретическое понимание, так и в практическую реализацию систем распознавания лиц в некооперативных средах. Продемонстрированные улучшения производительности в сложных условиях, в сочетании с практическими соображениями по развертыванию, обеспечивают основу для более надежных систем распознавания лиц в контекстах безопасности.

ЛИТЕРАТУРА

1. O.M. Parkhi, A. Vedaldi, and A. Zisserman, «Deep face recognition», in Proceedings of the British Machine Vision Conference, 2015, pp. 41.1–41.12.
2. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, «ArcFace: Additive angular margin loss for deep face recognition», in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2019, pp. 4690–4699.
3. S. Z. Li and A. K. Jain, Handbook of Face Recognition, 2nd ed. London: Springer-Verlag, 2011. 699 p.
4. G.B. Huang, M. Ramesh, T. Berg, and E. Learned-Miller, «Labeled faces in the wild: A database for studying face recognition in unconstrained environments,» Technical Report 07-49, University of Massachusetts, Amherst, 2007.
5. Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, «DeepFace: Closing the gap to human-level performance in face verification», in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 1701–1708.
6. F. Schroff, D. Kalenichenko, and J. Philbin, «FaceNet: A unified embedding for face recognition and clustering», in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2015, pp. 815–823.
7. X. Wang, X. Duan, and X. Bai, «Deep feature extraction and classification of hyperspectral images based on convolutional neural networks», IEEE Transactions on Geoscience and Remote Sensing, 2016;54(10):6232–6251. https://doi.org/10.1109/TGRS.2016.2584107
8. I.J. Goodfellow, J. Shlens, and C. Szegedy, «Explaining and harnessing adversarial examples», in International Conference on Learning Representations, 2015.
9. S. Dodge and L. Karam, «Understanding how image quality affects deep neural networks», in International Conference on Quality of Multimedia Experience, 2016, pp. 1–6.
10. S. Xie, R. Girshick, P. Dollár, Z. Tu, and K. He, «Aggregated residual transformations for deep neural networks», in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 1492–1500.
11. S. Woo, J. Park, J.-Y. Lee, and I. S. Kweon, «CBAM: Convolutional block attention module», in Proceedings of the European Conference on Computer Vision, 2018, pp. 3–19.
12. F.M. Carlucci, L. Porzi, B. Caputo, E. Ricci, and S.R. Bulò, «AutoDIAL: Automatic domain alignment layers», in Proceedings of the IEEE International Conference on Computer Vision, 2017, pp. 5077–5085.
13. M. Merler, N. Ratha, R. S. Feris, and J. R. Smith, «Diversity in faces», arXiv preprint arXiv:1901.10436, 2019.
14. X. Wang, S. Wang, J. Wang, H. Shi, and T. Mei, «Co-mining: Deep face recognition with noisy labels», in Proceedings of the IEEE/CVF International Conference on Computer Vision, 2019, pp. 9358–9367.
15. M. Huber, M. Schlitter, and R. Eidenberger, «RobustNet: Improving domain generalization in urban-scene segmentation via instance selective whitening», in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2020, pp. 11580–11590.
16. X. Zhang, S. Wang, J. Liu, and C. Tao, «Towards improving the robustness of deep neural networks by training with adversarial examples», IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 43, no. 3, pp. 888–901, 2021.
17. X. Cao, D. Wipf, F. Wen, G. Duan, and J. Sun, «A practical transfer learning algorithm for face verification», in Proceedings of the IEEE International Conference on Computer Vision, 2013, pp. 3208–3215.
18. A.K. Singh, P. Joshi, and G.C. Nandi, «Face recognition with liveness detection using eye and mouth movement», in International Conference on Signal Propagation and Computer Technology, 2014, pp. 592–597.
19. L. Best-Rowden and A.K. Jain, «Longitudinal study of automatic face recognition», IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 40, no. 1, pp. 148–162, 2018.
20. R. Geirhos, J.-H. Jacobsen, C. Michaelis, R. Zemel, W. Brendel, M. Bethge, and F.A. Wichmann, «Shortcut learning in deep neural networks», Nature Machine Intelligence, vol. 2, no. 11, pp. 665–673, 2020.

Журнал «Современная наука: актуальные проблемы теории и практики»