

Ю. Н. Ханбекова^{1✉}

Метод обнаружения атак с предъявлением фотографий в биометрических системах

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: yul2002@mail.ru

Аннотация. В статье описан метод обнаружения атак с использованием поддельных биометрических данных в задачах распознавания лиц. Актуальность заключается в том, что атаки предъявления являются одним из наиболее доступных и распространенных способов обхода биометрической аутентификации. Целью исследования является разработка метода, позволяющего повысить точность определения атаки в условиях плохого освещения на основе нейросетевой модели. Предложенный метод включает модуль предварительного улучшения освещения изображения, двухветвевую модель, в которой одна ветвь предназначена для извлечения признаков исходного изображения лица, а вторая – для извлечения текстурных признаков. Полученные признаки объединяются и подаются на вход блока бинарной классификации. В работе продемонстрировано, что совместное использование коррекции освещения, анализа признаков изображения и анализа текстурных особенностей позволяет повысить устойчивость метода к различным сценариям освещения и точность обнаружения атаки.

Ключевые слова: атаки предъявления, нейронная сеть, текстурные признаки, распознавание лиц, антиспуфинг, бинарная классификация

Yu. N. Khanbekova^{1✉}

Method for detecting photo presentation attacks in biometric systems

¹National Research Nuclear University MEPhI, Moscow, Russian Federation
e-mail: yul2002@mail.ru

Abstract. The article describes a method for detecting attacks involving spoofed biometric data in face recognition tasks. The relevance of the study lies in the fact that presentation attacks are among the most accessible and widespread ways of bypassing biometric authentication. The aim of the research is to develop a method that improves attack detection accuracy under poor lighting conditions based on a neural network model. The proposed method includes a module for preliminary image illumination enhancement and a dual-branch model, in which one branch is designed to extract features from the original facial image, while the other branch is intended to extract texture features. The extracted features are fused and fed into a binary classification block. The study demonstrates that the combined use of illumination correction, image feature analysis, and texture feature analysis makes it possible to improve the robustness of the method to various lighting scenarios and increase attack detection accuracy.

Keywords: presentation attacks, neural network, texture features, face recognition, anti-spoofing, binary classification

Введение

Современные информационные системы стали чаще внедрять использование биометрических методов идентификации личности, такие как отпечатки

пальцев, голос, лицо [1–3]. Одновременно с широким распространением биометрических технологий возникла новая угроза – спуфинг. Спуфинг – это попытка обмана системы путем предъявления поддельных данных. Появление данных атак стимулировало развитие отдельного направления – антиспуфинг [4].

В публикациях по теме антиспуфинга особое внимание уделяется применению методов глубокого обучения для определения визуальных признаков подделки изображения [1–5]. Несмотря на достигнутые результаты, остается ряд нерешенных вопросов: существующие методы не всегда обеспечивают достаточную точность распознавания фото атак при плохом освещении, когда часть информативных признаков скрыта. Многие подходы ориентированы на анализ общего изображения лица и не учитывают текстурные особенности, являющиеся метками поддельных данных.

Существенную значимость проблемы подтверждает нормативная база. Согласно ГОСТ Р 58624.1–2019 [6], наличие механизмов обнаружения атак на биометрическое предъявление является обязательным требованием при проектировании надежных биометрических систем [7–9]. Это подтверждает, что защита от спуфинг атак рассматривается не только как исследовательская задача, но и как необходимое условие практического внедрения биометрических решений. При этом антиспуфинг-модуль должен сохранять устойчивость к различным внешним факторам, таким как недостаточное освещение, изменение угла поворота головы, плохое качество камеры [10–13].

Целью работы является разработка метода обнаружения фото атак в условиях плохого освещения на основе нейросетевой модели, обеспечивающего повышение точности распознавания поддельных изображений лиц.

Предлагаемое решение

Предлагаемое решение основывается на совместном использовании предварительной коррекции освещения и двухветвевой нейросетевой архитектуры. Для надежного обнаружения атак предъявления недостаточно анализировать только общее изображение лица. Необходимо одновременно учитывать глобальные и текстурные признаки изображения. Глобальные признаки характеризуют визуальное представление лица. Текстурные артефакты могут содержать прямые признаки атаки: следы печати, муар, неестественную зернистость и др. Поэтому в разработанном методе используется архитектура, включающая две ветви обработки признаков: ветвь признаков изображения и ветвь текстурных признаков (рис. 1).

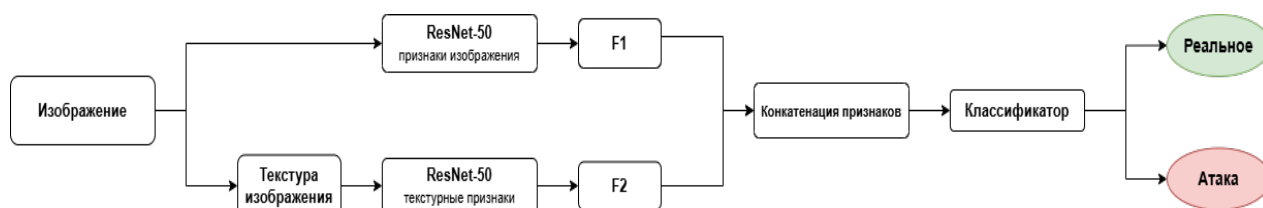


Рис. 1. Поточная диаграмма модели

Общий алгоритм работы метода включает несколько последовательных этапов. На первом этапе на вход системы подается изображение лица. Далее выполняется предварительная обработка изображения: нормализация размеров, приведение к заданному формату и коррекция освещения. После этого формируются два представления одного и того же входного кадра. Первое представляет собой улучшенное изображение лица, сохраняющее глобальные визуальные характеристики. Второе представление формируется на основе текстурного преобразования и предназначено для выделения локальных особенностей поверхности изображения. Далее каждое из этих представлений поступает в соответствующую ветвь нейронной сети, где происходит извлечение признаков. Полученные векторы признаков объединяются в единый вектор с помощью конкатенации. Объединенный вектор признаков подается в классификационный блок, который формирует итоговое решение об атаке (рис. 2).

Одной из составляющих предлагаемого решения является модуль предварительного улучшения освещения. Его назначение – это увеличение информативности признаков, значимых для задачи антиспуфинга. Отличительной чертой предлагаемого решения является сохранение локальных визуальных артефактов, указывающих на использование поддельного изображения. Разработанный модуль улучшения освещения ориентирован на селективную коррекцию темных участков при сохранении структуры изображения. На первом шаге оценивается распределение яркости входного изображения через L-канал пространства LAB и строится карта затемненных областей. Такая карта позволяет определить участки, в которых полезная информация скрыта из-за недостаточного освещения. На втором шаге изображение представляется как сочетание двух компонент: освещения и отражения, или текстуры. Дальнейшая коррекция применяется только к компоненте освещения, текстурная составляющая сохраняется исходной. На следующем этапе выполняется коррекция яркости. Коррекция выполняется как локально-переменная гамма-коррекция компоненты освещения. Для каждого пикселя строится карта гамма-параметра $\gamma(x,y)$: чем темнее участок, тем меньше γ и тем сильнее усиливается яркость. По сравнению с глобальным повышением яркости, здесь степень коррекции зависит от затемнения рассматриваемого участка. Чем ниже локальная освещенность, тем сильнее усиливается соответствующая область, но величина корректировки ограничивается так, чтобы не привести к пересвету и не разрушить естественное соотношение между соседними участками. Дополнительно применяется сдерживание слишком ярких областей, что позволяет уменьшить влияние пересветов и сделать распределение яркости более сбалансированным. После коррекции освещения итоговое изображение восстанавливается по Retinex-схеме.

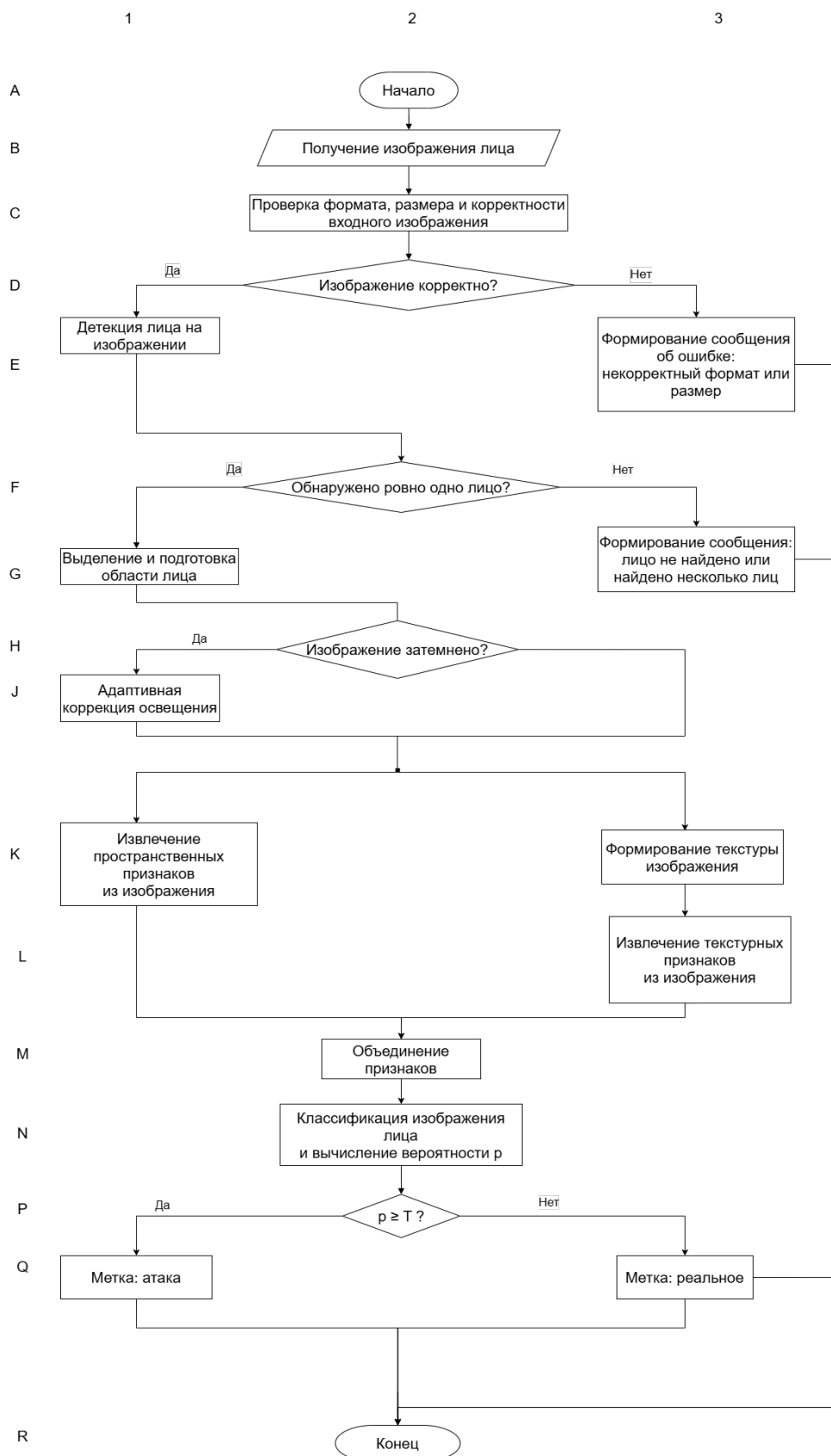


Рис. 2. Блок-схема алгоритма обнаружения атаки

Важным свойством модуля является то, что он не стремится удалить все блики и контрастные перепады, так как часть подобных эффектов может быть связана именно с признаками атаки.

Результаты

В ходе исследования было проведено тестирование разработанного метода обнаружения атак. В качестве базового варианта использовалась модель без модуля улучшения освещения и без разделения на две ветви признаков. Далее оценивалось влияние разработанного алгоритма улучшения освещения совместно с использованием двухветвевой архитектуры. В качестве основного показателя качества использовалась точность классификации. Результаты сравнительного эксперимента представлены в табл. 1.

Таблица 1. Сравнение точности моделей обнаружения атак

Вариант тестирования	Точность классификации, %
Базовая модель	88,3
Разработанный метод	98,5

Результаты тестирования подтвердили, что применение разработанного метода позволило повысить точность классификации с 88,3 % до 98,5 %. Количественное улучшение точности составило 10,2 %.

Заключение

В статье предложен метод обнаружения фото атак в биометрических системах распознавания лиц, основанный на использовании модуля улучшения освещения и двухветвевой нейросетевой архитектуры. Показано, что предварительная коррекция затемненных участков при сохранении локальных артефактов позволяет повысить информативность изображения для задачи антиспуфинга. Разработанный метод объединяет анализ глобальных признаков изображения и текстурных признаков. Предложенный подход может быть использован при создании модулей защиты биометрических систем, работающих в условиях нестабильного освещения.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Кудяева В.М., Федорова И.А., Ермаков А.В. Инновационные методы обнаружения спуфинг-атак на систему лицевой биометрии // Измерение, контроль, информатизация: Материалы XXIII Международной научно-технической конференции, Барнаул, 20 мая 2022 года / Под редакцией Л.И. Сучковой. – Барнаул: Алтайский государственный технический университет им. И.И. Ползунова – 2022. – С. 139-142.
2. Миронова Н.Г. Методы антиспуфинга в системах биометрической идентификации и верификации // Информационные технологии обеспечения комплексной безопасности в цифровом обществе: сборник материалов IV Всероссийской молодежной научно-практической конференции с международным участием, Уфа, 21–22 мая 2021 года. – Уфа: Башкирский государственный университет – 2021. – С. 43-51.

3. Минкин А.В., Каракеян А.С. Анализ методов face anti-spoofing для обеспечения безопасности биометрической аутентификации в условиях цифровизации // Журнал Современные наукоемкие технологии. – 2025. – № 9. С. 167-175.
4. К. Д. Русаков, А. А. Генов, С. Ш. Хиль Методика решения задачи антиспуфинга по ограниченному количеству фотографий // Программные продукты и системы. – 2020. – Т. 33 – №1. – С. 54-60.
5. Киба А.С., Фаворская М.Н. Обнаружение поддельных изображений лиц на основе глубокого обучения // Решетневские чтения: Материалы XXIV Международной научно-практической конференции, посвященной памяти генерального конструктора ракетно-космических систем академика М. Ф. Решетнева: в 2 частях, Красноярск, 10–13 ноября 2020 года. Том Часть 2. – Красноярск: Федеральное государственное бюджетное образовательное учреждение высшего образования "Сибирский государственный университет науки и технологий имени академика М.Ф. Решетнева" – 2020. – С. 403-404.
6. ГОСТ Р 58624.1–2019. Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура. – Москва: Стандартинформ, 2019. – 12 с.
7. Мудрич А. Б., Ежова К. В. Детектирование и распознавание лиц в системах видеонаблюдения // International Journal of Open Information Technologies. – 2024. – Т.12. – №3. – С. 82-84.
8. Частикова, В.А., Титова А.А., Войлова Д.О. Аналитический обзор методов идентификации личности на основе биометрических характеристик // Вестник Адыгейского государственного университета. Серия: Естественно-математические и технические науки. – 2022. – № 1(296). – С. 92-112. – DOI 10.53598/2410-3225-2022-1-296-92-112.
9. Е. А. Омеляненко, Е. А. Басыня, А. В. Сафронов Разработка системы контроля и управления доступом персонала в рудник на основе биометрической идентификации // Перспективное развитие науки, техники и технологий : Сборник научных статей VII-ой Международной научно-практической конференции, Курск, 13–14 октября 2017 года / Ответственный редактор А.А. Горохов. – Курск: Закрытое акционерное общество "Университетская книга", 2017. – С. 142-150.
10. Басыня, Е. А., А. В. Сафронов Разработка и исследование системы управления метаданными изображений // Актуальные проблемы электронного приборостроения АПЭП - 2016 : Труды XIII Международной научно-технической конференции. В 12-ти томах, Новосибирск, 03–06 октября 2016 года. Том Том 9. – Новосибирск: Новосибирский государственный технический университет, 2016. – С. 155-157.
11. Гусев Юрий Борисович Приватные биометрические криптосистемы: архитектура, математические основы и алгоритмы // Инновации и инвестиции. – 2025. – №2. – С. 424-429.
12. Денисова А. Ю., Федосеев В. А. Обнаружение атак на биометрическое предъявление на системы аутентификации лиц при помощи специальных устройств съемки // Компьютерная оптика. – 2022. – Т. 46. – №. 4. – С. 612-620.
13. Минкин А.В., Каракеян А.С. Анализ методов face anti-spoofing для обеспечения безопасности биометрической аутентификации в условиях цифровизации // Журнал Современные наукоемкие технологии. – 2025. – №. 9. – С. 167-175.

© Ю. Н. Ханбекова, 2026