ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

д.т.н. А.А. Орлова на диссертационную работу

Ефимова Юрия Сергеевича

«Методы детектирования подделок в биометрических системах на мобильном устройстве»,

представленную на соискание ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики»

Актуальность темы

Идентификация человека методами биометрического распознавания играет большую роль в современном обществе. Существенная часть банковских транзакций требует высокого уровня безопасности, достигаемого в том числе за счёт применения биометрических технологий. Распространение и улучшение характеристик мобильных устройств привело к росту количества осуществляемых с их помощью банковских операций. При этом значительная часть систем распознавания подвержена взлому при помощи поддельных биометрических характеристик, которые также называют спуфинг-атаками. Мобильный сценарий применения биометрических технологий существенно ограничивает возможности противодействия попыткам подделывания. Существенно изменчивые условия регистрации изображений в системах распознавания по лицу и радужке, распространённых в современных мобильных устройствах, влияют на качество входных данных, а ограниченные вычислительные ресурсы устройств затрудняют внедрение сложных методов. Данные ограничения не позволяют достичь целевых показателей точности обнаружения подделок с использованием существующих методов.

В диссертации Ю.С.Ефимова предлагается набор методов и алгоритмов, которые позволяют осуществлять защиту от подделывания при распознавании по лицу и радужной оболочке глаза на мобильном устройстве в режиме реального времени и достичь показателей точности детектирования спуфинг-атак, сопоставимой с немобильными приложениями технологии и достаточной для внедрения в современные смартфоны. Таким образом, тема диссертации, без сомнения, является актуальной.

Содержание работы

Диссертация состоит из введения, обзора литературы, пяти глав, заключения и списка литературы.

Во введении обосновывается актуальность проводимых исследований, научная новизна и практическая ценность работы, сформулированы цели, задачи и основные положения, выносимые на защиту.

Первая глава содержит обзор биометрических методов распознавания и подходов к построению систем защиты от подделок. Сформулированы общие требования к алгоритмам обнаружения подделок для мобильных систем распознавания с учетом специфики их применения пользователем. Приведены преимущества и недостатки наиболее распространённых в мобильных приложениях модальностей изображения лица и радужки с точки зрения их уязвимости к подделыванию и внутриклассовой изменчивости входных данных в зависимости от условий съёмки.

Во второй главе подробно рассмотрены особенности защиты от подделок для систем распознавания по лицу в мобильных устройствах с единственной фронтальной камерой, среди которых разнообразные по освещённости и видимым характеристикам сценарии съёмки и применения, а также ограниченная производительность. Произведена классификация способов подделывания по типам физических артефактов, квалификации взломщика и доступности биометрической информации. Предложен алгоритм, позволяющий определять живость изображения лица пользователя мобильного устройства в режиме реального времени. В главе также приводится описание компонент алгоритма, построенных с целью обнаружения тех или иных характерных наблюдаемых артефактов подделывания. В завершении приводятся результаты оценки точности и быстродействия для предложенного метода.

В третьей главе рассматривается задача защиты от подделывания для мобильной системы распознавания по лицу с применением стереоинформации, извлекаемой при помощи пары камер видимого света с малым стереобазисом, характерным для мобильных устройств. Предложен алгоритм определения живости лица по стереоизображению, построенный на применении свёрточной нейронной сети. Для повышения обобщающей способности и регуляризации внутренних представлений сети с учётом специфики стереоинформации предложена новая функция потерь, позволяющая достичь наилучшего качества решения. Приведены оценки производительности метода на мобильном устройстве и точности детектирования подделок, в том числе на открытой базе данных стереоизображений лиц.

Четвёртая глава посвящена обнаружению границ радужки на изображении, в том числе низкого качества, путём аппроксимации их окружностями с помощью нейронной сети. Дан обзор существующих методов с упором на подходы, основанные на применении свёрточных нейросетей. Приводится описание архитектуры сети, предложенной автором для решения задачи регрессии параметров аппроксимирующих окружностей путём сведения к решению задачи классификации. Приведено описание эксперимента, результаты сравнения по точности выделения с существующими аналогами и оценки по скорости выполнения на мобильном устройстве.

В пятой главе рассматривается задача обнаружения попыток подделывания радужки. Приводится обзор и классификация подходов к защите от подделывания, предложены новые, ранее не рассматриваемые способы создания искусственных радужек. Затем приводится описание предлагаемого алгоритма, построенного в виде свёрточной нейронной сети особой архитектуры. Предлагаемая модель позволяет обеспечивать защиту как от распространённых и описанных в научных трудах видов атак, так и от ранее не рассматриваемых. В заключении приводятся оценки по скорости и точности обнаружения подделок, а также сравнение с известными из литературы подходами.

В заключении представлены основные результаты работы.

Основные результаты.

В рамках диссертационной работы Ю.С. Ефимова были получены следующие основные результаты:

1. Предложена новая многостадийная структура алгоритма защиты от подделывания лица для мобильных устройств с единственной фронтальной камерой видимого спектра излучения (глава 2, параграф 2.4.1, рис. 2.3), позволяющая до применения вычислительно сложных алгоритмов обнаруживать подделки с помощью комбинации методов раннего обнаружения характерных артефактов и дефектов и использующая для повышения стабильности в условиях изменчивых параметров окружения данные экспозиции камеры и вспомогательных сенсоров устройства.
2. Разработан и протестирован новый метод определения живости лица на стереоизображении, извлекаемом парой камер видимого спектра излучения с малым стереобазисом, при помощи классификатора в виде сверточной нейронной сети, обучаемой с применением новой функции потерь (глава 3, параграф 3.2).
3. Разработана новая архитектура нейросетей для аппроксимации границ радужки на изображении глаза окружностями (глава 4, параграф 4.2, таблица 4.1).
4. Предложена новая архитектура свёрточной нейросети (глава 5, параграф 5.2, таблица 5.1), позволяющая обеспечивать защиту от известных и новых видов атак.

Научная новизна и обоснованность результатов.

Предлагаемые подходы являются новыми. Научные положения, выводы и рекомендации, сформулированные в диссертации, являются в достаточной степени обоснованными и достоверными. Это подтверждается глубокой проработкой литературы по теме диссертации, наличием докладов на международных и всероссийских конференциях по

анализу данных и биометрии, а также внедрением результатов в реальное практическое использование. Научные положения и выводы подкреплены фактическими данными, полученными по результатам многочисленных экспериментов, представленных в виде рисунков и таблиц.

Значимость полученных результатов

В работе достаточно глубоко исследованы особенности обнаружения подделок при распознавании человека по лицу и радужной оболочке глаза при помощи мобильного устройства, предложен набор высокопроизводительных методов и алгоритмов, позволяющих осуществлять построение устойчивых систем защиты от подделывания на мобильном устройстве. Показательным признаком значимости полученных результатов является их применение в серийных коммерческих мобильных устройствах, выпускаемых компанией Samsung Electronics Co. Ltd. в период с 2018 по 2021 гг.

Замечания

1. Во второй главе указана оценка качества многостадийного решения, но не приведено сравнение с описанными в литературе аналогами, если таковые имеются.
2. Во второй главе дана общая оценка производительности предлагаемого метода, и не дана более подробная оценка для составляющих его компонент.
3. В четвертой главе отсутствует ссылка на один из используемых наборов данных.
4. Для приведённого в пятой главе сравнения предложенного метода с известными из литературы аналогами использован единственный набор данных.
5. В некоторых главах (например, в третьей) по тексту разнесены особенности предложенного метода. Текст диссертации был бы лучше структурирован, если бы эти особенности были сформулированы в начале главы (описания), а далее по тексту приводилась бы соответствующая ссылка.
6. Не все названия разработанных методов во введении соответствуют названиям в основном тексте диссертации.
7. В формуле для α_{LR} на стр. 67 не учтена ситуация деления на ноль.
8. В заключении диссертации отсутствуют числовые показатели эффективности разработанных методов и алгоритмов.

Заключительная оценка

Указанные замечания не снижают общую положительную оценку выполненной автором работы. Диссертация представляет собой завершенную научно-исследовательскую работу. Структура и содержание диссертации соответствуют целям и задачам исследования. Основные результаты изложены в семнадцати публикациях, пять из которых входят в перечень рекомендованных ВАК РФ. Результаты докладывались на Всероссийских и международных конференциях.

Диссертационная работа Ефимова Ю.С. «Методы детектирования подделок в биометрических системах на мобильном устройстве» соответствует требованиям ВАК РФ (пп. 9-14 «Положения о присуждении ученых степеней», утвержденного постановлением Правительства Российской Федерации от 24 сентября 2013 г. № 842), предъявляемым к диссертациям на соискание ученой степени кандидата технических наук по специальности 05.13.17 – «Теоретические основы информатики», а её автор, Ефимов Ю.С., заслуживает присуждения ему ученой степени кандидата технических наук по данной специальности.

Официальный оппонент

Заведующий кафедрой физики и прикладной математики Муромского института (филиала) ФГБОУ ВО «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых», доктор технических наук, доцент

Орлов Алексей Александрович

602264, Владимирская область, г. Муром, ул. Орловская, д. 23
Телефон: 8-(49234) 77-1-24
E-mail: alexeyalexorlov@gmail.com
Научная специальность: 05.13.01 Системный анализ, управление и обработка информации

Подпись доктора технических наук,
доцента Орлова А.А. заверяю:
Директор МИ ВлГУ А.Л. Жизняков

«22» 08 2022г.